Advanced URL Filtering

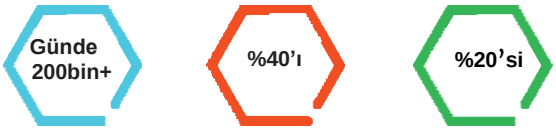
En Gelişmiş Web Koruması

Web'i Gerçek Zamanlı Koruma

Uygulamalar buluta taşındıkça ve mobil çalışma modeli yaygınlaştıkça, firmalar için web güvenliğini sağlamak daha önemli hale geliyor. Günümüzde, kimlik avı ve dosyasız saldırılar gibi web tabanlı saldırıların hem sayısı hem de karmaşıklığı artıyor. Buna karşılık çoğu web güvenliği sağlayan çözüm, bilinen zararlı web sayfalarını veri tabanlarında saklamaktan öteye gidemiyor.

Palo Alto Networks Advanced URL Filtering, günümüzde işletmeler için, en gelişmiş web korumasını sağlar. Advanced URL Filtering, Palo Alto Network'ün bilinen URL Filtering özelliği ile ML tabanlı geliştirilmiş gerçek zamanlı web trafiği koruma mimarisini birleştirdi.

Artık yeni kötü amaçlı ve hedefli web tabanlı tehditleri otomatik olarak algılayabilir ve önleyebilirsiniz. Gerçek zamanlı korumaya hoş geldiniz!



*Geleneksel veritabanlarının önceleyemediği gerçek zamanlı önlenen saldırıların sayısı günde 200.000'den fazla.

*Önlenen URL'lerin %40'ı başka hiçbir güvenlik sağlayıcısı tarafından bilinmiyor.

*Önlenen kimlik avı saldırılarının %20'si başka biçbir güvenlik sağlayıcısı tarafından bilinmiyor.

Advanced URL Filtering, Diğerlerinin Yapmadığı Saldırıları Önler.

Şekil 1: Advanced URL Filtering, günümüzde kurumsal ağlara yönelik en çok zarar veren web tabanlı saldırıları tespit eder.

Advanced URL Filtering Farkı

Bulutta yerleşik olan Advanced URL Filtering, kimlik avı, kötü amaçlı yazılım, komuta ve kontrol (C2) gibi tehditlere karşı web erişimini koruma altına almak için, Palo Alto Networks Yeni Nesil Güvenlik Duvarınız (NGFW) ile lokal olarak çalışan bir lisans hizmetidir. Bu hizmet, URL'leri gerçek zamanlı olarak analiz etmek ve aynı zamanda web trafiğinin tam kontrolü için NGFW politikanıza kolayca ekleyebileceğiniz iyi veya kötü niyetli kategorilere ayırmak ,yani sınıflandırmak için ML kullanır.

Bu kategoriler, NGFW platformunda tamamlayıcı özellikleri tetikleyerek, hedeflenen SSL şifre çözme ve gelişmiş günlük kaydı gibi ek koruma katmanları da sağlar.Advanced URL Filtering, kendi analizinin yanı sıra, kötü amaçlı sitelere karşı korumaları otomatik olarak güncellemek için WildFire® ve diğer kaynaklardan paylaşılan analizleri kullanır.

Advanced URL Filtering kullanıcılarına şunları sağlar:

- Bilinen tehditleri durduran URL lisansı ve sektördeki ilk inline web koruma motorumuzla web tabanlı saldırılara karşı üstün koruma sağlar. Advanced URL Filtering ile, içerik tarayıcılardan gizlendiğinde bile, yeni kötü amaçlı URL'leri gerçek zamanlı olarak sınıflandırabilir ve aynı zamanda engelleyebilirsiniz.
- Kullanıcılara, risk derecelendirmelerine ve içerik kategorilerine göre güvenlik eylemlerini otomatikleştirmenize yarayan özel ayarlanmış kontroller ve politika ayarları aracılığıyla **web trafiğinizin tam kontrolünü sağlar.**
- Palo Alto Networks platformu aracılığıyla web koruması sağlayarak **maksimum operasyonel verimlilik sunar.**

Faydaları

- **Yeni kötü amaçlı siteleri engeller.** Advanced URL Filtering, daha önce hiç görülmemiş kötü amaçlı URL'leri, ağınıza ve son kullanıcılarınızı zarar verme ihtimali doğmadan milisaniyeler içinde kategorize eder ve engeller.
- **Tutarlı güvenlik politikalarından ve profillerinden yararlanırsınız.** Advanced URL Filteringi donanım, sanal ortamlarda veya bulutta devamlı olarak uygulanan politikalar ve güvenlik profilleri ile kullanabilirsiniz.
- **Güvenlik silolarını ortadan kaldırarak, kullanıcıları güvende tutarsınız.** Noktasal çözümlere kıyasla %30 daha hızlı güvenlik elde etmenize yardımcı olur.
- **Operasyonel maliyetleri en aza indirirsiniz.** Palo Alto Networks bulut güvenlik hizmetleri, bağımsız çözümlere duyulan ihtiyacı azaltarak 3 yılda 9,9 milyon USD tasarruf sağlıyor.[1]
- **Kimlik avına karşı koruma.** Kimlik avını gerçek zamanlı olarak durdurarak kuruluşunuzu bilinen ve bilinmeyen kimlik avı sitelerinden korur.

*** Uyumluluk ve kolay kullanımı destekler.** Kuruluşunuzun şirket içi, sektör ve devlet düzenleyici politikalarıyla uyumlu kalmasını sağlar.

TEMEL ÖZELLİKLER:

Buna ek olarak, kötü niyetli URL'lerin %40'ı bilinen etki alanlarından gelir, çünkü saldırganlar güvenilir olduğu düşünülen web sitelerine tehditler yerleştirir. URL'ler çoğunlukla iyi niyetliden kötü niyetliye kadar değişik risk düzeylerindedir ve mevcut çözümünüz bu riskleri sürekli olarak analiz etmedikçe, altyapınız saldırılara açık olacaktır.

Günümüzde firmalar, artık sadece statik veya yavaş güncellenen veri tabanlarına güvenemez. Bu yüzden, yeni bir yaklaşım gereklidir. Advanced URL Filtering, yeni tehditleri kullanıcılarınıza ulaşmadan önce algılama ve engelleme özelliğiyle web korumasını bir üst seviyeye taşır. Bulut tabanlı inline makine öğrenimi (ML) sayesinde gerçek web trafiğini analiz eder, kötü amaçlı URL'leri kategorize eder ve kuruluşunuza zarar verme şansı bulamadan milisaniyeler içinde engeller. Makine öğrenimi modellerimiz sık sık yeniden öğrenme yaparak yeni web tabanlı tehditlere karşı en güncel algılama istihbaratını sağlar. Bu arada, genişletilebilir bulut tabanlı mimarimiz, anında en son yenilikçi algılama modüllerinden yararlanmanızı sağlar. Çevrimdışı taramaya ve güncellenmesi çok uzun süren veri tabanlarına olan güvenin ötesine geçmenin zamanı geldi. Advanced URL Filtering, bu önlemi alarak, sektörde daha önce hiç görülmemiş web tabanlı tehditleri tespit edip gerçek zamanlı olarak önleyebilen ilk inline web koruma motorunu sunar.

Anti-Evasion

Günümüzde saldırganlar, güvenlik önlemlerini zorlayıcı alternatifler bulmaktadır ve şu anda karanlık ağda satılan kimlik avı kitlerinin %87'si en az bir tür kaçınma tekniği içeriyor. Gizleme adı verilen bu tekniklerin en yaygını, birçok web güvenlik çözümünün herhangi bir tehdidin var olup olmadığını belirlemek için yalnızca web sayfası içeriğinin çevrimdışı olarak taranmasına dayandığı gerçeğinden yararlanır. Saldırganlar, güvenlik şirketlerine ait olduğunu bildikleri belirli IP adreslerinden ve ana bilgisayarlardan gelen bağlantıları etkin bir şekilde engelleyebilir veya onları iyi niyetli içeriğe yönlendirebilir. Advanced URL Filtering, canlı web trafiğindeki URL'i analiz etmek için web sayfası taramasının ötesine geçerek saldırganları belirler ve kaçınma tekniklerinin arkasına sığınan kötü amaçlı siteleri tespit eder.

Kimlik Avı Koruması

En eski taktiklerden biri olan kimlik avı, kurumsal firmalar için zorluk oluşturmaya devam ediyor. Her 20 saniyede bir3 yeni bir kimlik avı sitesi açılmaktadır ve kimlik avı, bildirilen güvenlik olaylarının % 80'inden fazlasını ve başarılı ihlallerin %22'sini teşkil etmektedir.5 Dakikalar içinde yeni kimlik avı siteleri kurulup kapatılabildiği göz önüne alındığında, kimlik avı süreklilik arz eden bir tehdittir. Advanced URL Filtering sayesinde, bilinen milyonlarca kimlik avı sayfasından korunursunuz, ancak yeni kimlik avı sayfalarını ilk kurbanlarını talep etmeden önce anında ve doğru bir şekilde tespit etmek de çok önemlidir.

En gelişmiş kimlik avı korumasını sağlamak için aşağıdakiler dahil olmak üzere yenilikçi algılama özelliklerini birleştiriyoruz:

- Daha önce hiç görülmemiş kimlik avı saldırılarının gerçek zamanlı tespit edilmesi için inline ML tabanlı URL analizi
- Sektörün tek gerçek zamanlı kimlik bilgisi hırsızlığı önlemesi
- ML tabanlı görüntü analizi
- Yeni kaydedilmiş domain analizi
- Kimlik avı ve kötü amaçlı yazılım için gelişmiş JavaScript algılama
- Kimlik avı yeniden yönlendirme zinciri analizi
- Sahte CAPTCHA etkileşim analizi

Web Trafiğinin Tam Kontrolü

Web politikası basitçe, güvenlik duvarı politikanızın bir ekidir. Palo Alto Networks NGFW' niz, URL kategorilerini belirlemek, risk derecelendirmeleri atamak ve tutarlı politika uygulamak için Advanced URL Filtrering kullanır. Birden fazla URL kategorisi ve risk derecelendirmesini, tek bir politika seti aracılığıyla sağlayabilirsiniz. Bu da, basitleştirilmiş yönetime ve web trafiğinin ayrıntılı kontrolüne olanak tanır. Kimlik avı saldırılarında, kötü amaçlı yazılım dağıtım araçlarının tesliminde veya C2'de kullanılabilecek tehlikeli siteleri engellerken, .çalışanların iş için ihtiyaç duydukları web kaynaklarına erişme özgürlüğü sağlayabilirsiniz.

Operasyonel Verimlilik

Palo Alto Networks ile, web koruması sağlayarak güvenlik yatırımınızın toplam maliyetini azaltır ve operasyonel verimliliği en üst seviyeye çıkarırsınız. Bulut mimarisi sayesinde, Advanced URL Filtering, web koruması için ek donanımları devreye alma ve yönetme ihtiyacını ortadan kaldırır; bunu NGFW aracılığıyla açmanız yeterlidir. Bulut tarafından sağlanan güvenlik hizmetlerimiz, bağımsız çözümlere duyulan ihtiyacı azaltarak üç yılda 9,9 milyon USD tasarruf sağlarken, riski de %45 oranında azaltır. [6] Her güvenlik özelliğinin bir sonrakini iyileştirdiği bir platform kullanarak, noktasal çözümlere kıyasla %30 daha hızlı uygun güvenlik durumu elde edebilirsiniz.

Palo Alto Networks Güvenlik Lisanslarının Gücü

Günümüzde, siber saldırıların sayısı, etki alanı ve karmaşıklığı artmıştır. Bu, kuruluşların güvenlik ekipleri için iş yüklerini artırmadan veya iş verimliliğini etkilemeden ağlarını korumalarını sağlar. Sektör lideri NGFW platformumuzla sorunsuz bir şekilde entegre olan bulut tarafından sağlanan güvenlik lisanslarımız ihtiyacınız olan, korumayı sağlar. Palo Alto Networks güvenlik çözümleri sadece bugün değil, firmaların geleceği için de onların yanındadır.

1. "2019 Webroot Threat Report," (Webroot Tehdit Raporu) Webroot, 22 Şubat 2019, https://www-cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf.
2. "Mobile Threat Landscape Report 2020" (Mobil Tehdit Manzara Raporu), Wandera, 6 Mayıs 2021'de erişildi, https://www.wandera.com/mobile-threat-landscape.
3. "En önemli siber güvenlik gerçekleri, rakamları ve istatistikleri", IDG'den CSO, 9 Mart 2020,https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.
4. "2020 Veri İhlali Araştırma Raporu," Verizon, 3 Mayıs 2021'de erişildi, https://enterprise.verizon.com/resources/reports/dbir.
5. Forrester Toplam Ekonomik Etki çalışması.

Gelişmiş bir güvenlik deneyimi yaşamak ve pazar lideri özelliklerden yararlanmak için, Advanced URL Filtering'i veya aşağıdaki lisansları ihtiyacınıza göre tercih edebilirsiniz.

- **Threat Prevention**: Tek bir geçişte tüm trafikte bilinen tüm tehditleri otomatik olarak önlemek için geleneksel IPS'in ötesine geçin.
- **WildFire**: Sektör lideri bulut tabanlı analiz ile bilinmeyen kötü amaçlı yazılımların otomatik olarak algılanması ve önlenmesiyle dosyaların güvende olduğundan emin olun.
- **DNS Security**: Altyapınızda herhangi bir değişiklik yapmadan C2 ve veri hırsızlığı için DNS kullanan saldırıları kesintiye uğratın.
- **IoT Security**: Sektörün ilk anahtar teslimi (IoT) güvenlik çözümü ile kuruluşunuz genelinde IoT ve OT cihazlarını koruyun.
- **GlobalProtect™**: İlgili ortamınızın her yerinde tutarlı güvenlik sağlamak için NGFW özelliklerini uzak kullanıcılarınıza genişletin.

Operasyonel Faydalar

Advanced URL Filtering lisansı ile,

- Threat Prevention ve WildFire ile sıkı entegrasyonun yanı sıra kullanımı kolay uygulama ve kullanıcı tabanlı politikalarla sınıfının en iyisi web güvenliğinden yararlanın.
- **Web trafiğinde tam kontrol sağlayın.** Şüpheli siteler için seçici TLS/ SSL şifre çözme gibi gelişmiş güvenlik eylemlerini otomatik olarak tetiklemek için URL kategorilerini kullanın.
- **Güvenliğinizi otomatikleştirin**Politika, URL kategorilerine otomatik olarak uygulandığı ve analist müdahalesi gerektirmediği için zamandan tasarruf edin.
- **Kullanıcı ve URL etkinliği hakkında bilgi edinin.**BT departmanınızın, önceden tanımlanmış veya tamamen özelleştirilmiş bir dizi rapor aracılığıyla URL filtreleme ve ilgili web etkinliği hakkında görünürlük kazanmasını sağlayın.

Tablo 1: Advanced URL Filtering Özellikleri

Özellik	Açıklama
Inline Gerçek Zamanlı Web Tehdidi Önleme	Gerçek web trafiğini analiz etmek, kötü amaçlı URL'leri gerçek zamanlı olarak kategorilere ayırmak ve engellemek için bulut tabanlı inline ML kullanır. Makine öğrenimi modelleri sık sık yeniden tasarlanarak yeni ve gelişen, daha önce görülmemiş tehditlere (ör. kimlik avı, açıklardan yararlanma, dolandırıcılık, C2) karşı koruma sağlar.
Kaçınma Önlemleri	Gizleme sistemi, sahte CAPTCHA'lar ve HTML karakter kodlaması gibi kaçamak tekniklere karşı koruma sağlar.
URL Veri tabanı	Statik, dinamik, makine öğrenimi ve insan analizinin bir kombinasyonu aracılığıyla kategorize edilen yüz milyonlarca bilinen kötü niyetli ve iyi niyetli URL'yi barındırır.
İçerik Kategorileri	Web sitelerini site içeriğine, özelliklerine ve güvenliğine göre sınıflandırır ve 70'den fazla iyi niyetli ve kötü niyetli içerik kategorisini içerir.
Risk Derecelendirmeleri	Riski belirlemek için URL'leri çeşitli faktörlere göre puanlar. Bu güvenlik odaklı URL kategorileri, değişen düzeylerde risk oluşturan ancak kötü niyetli olarak onaylanmayan siteler için hedefli şifre çözme ve uygulama sağlayarak saldırı yüzeyinizi azaltmanıza yardımcı olabilir.
Çoklu Kategori Desteği	Bir URL'yi 4 adete kadar kategorilere ayırarak esnek politikaya ve özel kategorilerin oluşturulmasına olanak tanır.
Özel Kategoriler	Kategorileri ve ilkeleri kuruluşunuzun ihtiyaçlarına göre uyarlamanıza olanak tanır. Advanced URL Filtering, tanımlanmış bir kategoriler kümesi kullansa da, farklı kuruluşların risk toleransı, uyumluluk, düzenleme veya kabul edilebilir kullanım konusunda farklı ihtiyaçları olabilir. Gereksinimlerinizi karşılamak ve uyumlulukla ilgili ilkeleri düzenlemek için yöneticiler, mevcut birden çok kategoriyi birleştirerek yeni özel kategoriler oluşturabilir.
Gerçek Zamanlı Kimlik Hırsızlığı Koruması	Sitenin URL kategorisine göre kullanıcıların kendi kurumsal kimlik bilgilerini gönderebileceği siteleri kontrol ederek kimlik bilgisi hırsızlığını tespit eder ve önler. Bu, kullanıcıların gerçek zamanlı olarak güvenilmeyen sitelere kimlik bilgilerini göndermelerini engellemenize ve yine de kullanıcıların yalnızca kurumsal ve onaylanmış sitelere kimlik bilgilerini göndermelerine izin vermenize olanak tanır.
Kimlik Avı Görüntü Algılama	Kimlik avı girişimlerinde yaygın olarak kullanılan markaları taklit edip etmediklerini belirlemek amacıyla web sayfalarındaki görüntüleri analiz etmek için makine öğrenimi modellerini kullanır.
Kriter Eşleştirme	URL kategorilerine veya ölçütlerine dayalı olarak birden çok politika eylemi türü belirlemenize olanak tanır. Politika örnekleri, siteleri engellemenin veya sitelere izin vermenin ötesinde, seçici SSL şifre çözme, gelişmiş günlük kaydı, indirmeleri engelleme veya kimlik bilgilerinin gönderilmesini engellemeyi içerebilir.

Tablo 1: Advanced URL Filtering Özellikleri (devamı)	
Özellik	**Açıklama**
Seçici SSL Şifre Çözme	Hedeflenen şifre çözme ile riski daha da azaltmanıza yardımcı olur. TLS/SSL ile şifrelenmiş web trafiğinin seçici olarak şifresini çözmek için politikalar oluşturulabilir, bu da sizi veri gizliliği düzenlemeleriyle uyumlu tutarken potansiyel tehditlere karşı görünürlüğü en üst düzeye çıkarır. Belirli URL kategorileri (örneğin, sosyal ağ, web tabanlı e-posta, içerik dağıtım ağları) şifre çözme için atanabilirken, diğer site türlerine (örneğin, hükümetlerin, bankacılık kurumlarının, sağlık hizmeti sağlayıcılarınınkiler) yapılan ve bu sitelerden yapılan işlemler şifreli kalacak şekilde belirlenebilir. Yüksek veya orta risk derecelerine sahip geçerli içerik kategorileri için şifre çözmeyi sağlayan basit politikalar uygulayabilirsiniz. Seçici şifre çözme, şirket politikaları veya harici düzenlemeler tarafından belirlenen gizli trafik parametrelerine uyarken optimum güvenlik duruşu sağlar.
Çeviri Sitesi Filtreleme	Politikaları atlatmanın bir yolu olarak dil çevirisi web sitelerine (ör. Google Çeviri) girilen URL'lere URL Filtreleme politikaları uygular.
Arama Motoru Önbelleğe Alınmış Sonuçları Önleme	Son kullanıcılar web aramalarının ve internet arşivlerinin önbelleğe alınmış sonuçlarını görüntülemeye çalıştığında URL Filtreleme politikalarını uygular.
Güvenli Arama Yaptırımı	Kullanıcıların arama sonuçlarında uygunsuz içeriğin görünmesini engellemenize olanak tanır. Bu özellik etkinleştirildiğinde, yalnızca en katı güvenli arama seçenekleri ayarlanmış Google, Yandex, Yahoo veya Bing aramalarına izin verilir ve diğer tüm aramalar engellenebilir.
Özelleştirilebilir Son Kullanıcı Bildirimleri	Yöneticilerin, özel bir engelleme sayfası kullanarak kullanıcıları bir ihlal konusunda bilgilendirmesine olanak tanır. Bu sayfalar içerisinde, bir uyarı sunma ve kullanıcının devam etmesine izin verme veya bir politika istisnası oluşturan yapılandırılabilir bir parola gerektirme seçenekleri bulunabilir.
Çok Dilde Destek	41 dilde tarama ve analizi destekler.
Raporlama	Bir dizi önceden tanımlanmış veya tamamen özelleştirilmiş URL Filtreleme raporu aracılığıyla Gelişmiş URL Filtreleme ve ilgili web etkinliğine ilişkin görünürlük sağlar.

Tablo 2: Gizlilik ve Lisans Özeti	
Advanced URL Filtering Lisans ile Gizlilik	
Güven ve Gizlilik	Palo Alto Networks, hassas veya kişisel olarak tanımlanabilir bilgilere yetkisiz erişimi önlemek için katı gizlilik ve güvenlik kontrollerine sahiptir. Güvenlik ve gizlilik için endüstri standardı en iyi uygulamaları uyguluyoruz. Daha fazla bilgiyi gizlilik veri sayfalarımızda bulabilirsiniz.
Lisanslama ve Gereksinimler	
Gereksinimler	Palo Alto Networks Advanced URL Filtering lisansını kullanmak için, PAN-OS 9.0 veya sonraki bir sürümünü çalıştıran Palo Alto Networks Yeni Nesil Güvenlik Duvarlarına (NGFW) ihtiyacınız olacaktır.
Önerilen Ortam	Kötü amaçlı yazılım, grayware, kimlik avı, kimlik hırsızlığı ve C2 harici bağlantı gerektirdiğinden, İnternet'e yönelik herhangi bir konumda dağıtılan Palo Alto Networks Yeni Nesil Güvenlik Duvarları(NGFW) ile Advanced URL Filtering'i kullanın.
Advanced URL Filtering Lisansı	Advanced URL Filtering, Palo Alto Networks Yeni Nesil Güvenlik Duvarları (NGFW) için entegre, bulut tabanlı bir lisanstır. Firewall Flex'in bir parçası olarak da mevcuttur.

Detaylı bilgi almak ve demo talebinde bulunmak için, bizimle iletişime geçebilirsiniz

PanSales_TR@exclusive-networks.com