Palo Alto Networks Yeni Nesil Güvenlik Duvarına Genel Bakış

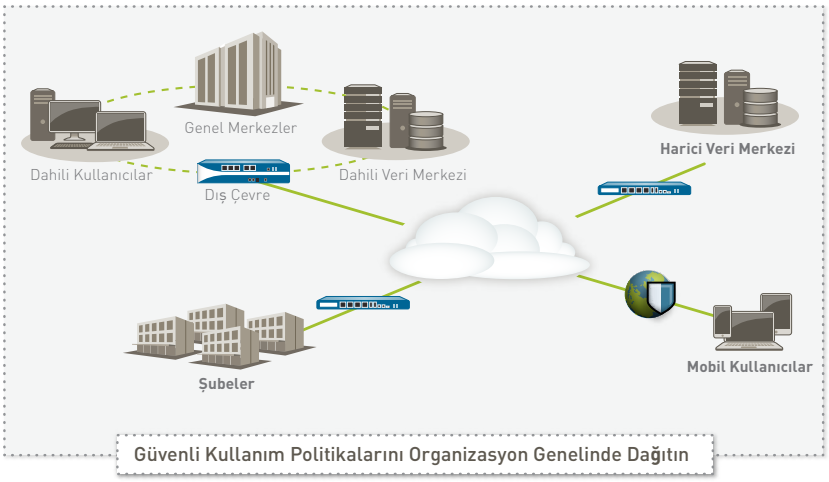
Uygulama ve tehdit dünyasında, kullanıcı davranışlarında ve ağ altyapılarında oluşan önemli farklılıklar, port ve protokol bilgisini esas alan klasik güvenlik duvarlarının bir zamanlar sağladığı güvenliği sürekli olarak zayıflatmış bulunmaktadır. Artık kullanıcılar, işlerinin gereği olarak, birçok farklı cihaz türünü kullanarak her türlü uygulamaya erişim sağlamaktadır. Bunun yanı sıra veri merkezlerinin genişlemesi, sanallaştırma, mobilite ve bulut tabanlı servisler gibi unsurlar, bir yandan uygulamalara erişim sağlanırken diğer yandan da ağların nasıl korunacağı konusunun yeniden düşünülmesi gerektiğini ortaya koymaktadır.

Bu durum karşısında güvenlik duvarına ek olarak önerilen klasik çözümler arasında, işin yapılmasını engelleyebilecek olan, bütün uygulama trafiğinin yalnızca sayısı sürekli artan bir nokta teknolojisi listesi üzerinden yapılması ya da aynı oranda kabul edilemez iş ve güvenlik risklerine neden olan, tüm uygulamalara izin verilmesi seçenekleri sayılabilir. Burada üstesinden gelmeniz gereken güçlük, klasik port ve protokol bilgisini esas alan güvenlik duvarının, uygulamaların son derece sıkı bir biçimde engellenmesine karşın yine de her iki yaklaşıma karşı bir seçenek oluşturmamasıdır. Her şeyin engellenmesi ile her şeye izin verilmesi seçenekleri arasında bir denge tutturmak için uygulama kimliği, uygulamayı kimin kullandığı ve içerik türü gibi yapılan işe ilişkin unsurları güvenlik duvarının ana trafik sınıflandırma ölçütü olarak kullanarak uygulamaları güvenli kılmanız gerekir.

Uygulamaları Güvenli Kılmanın Temel Gereksinimleri:

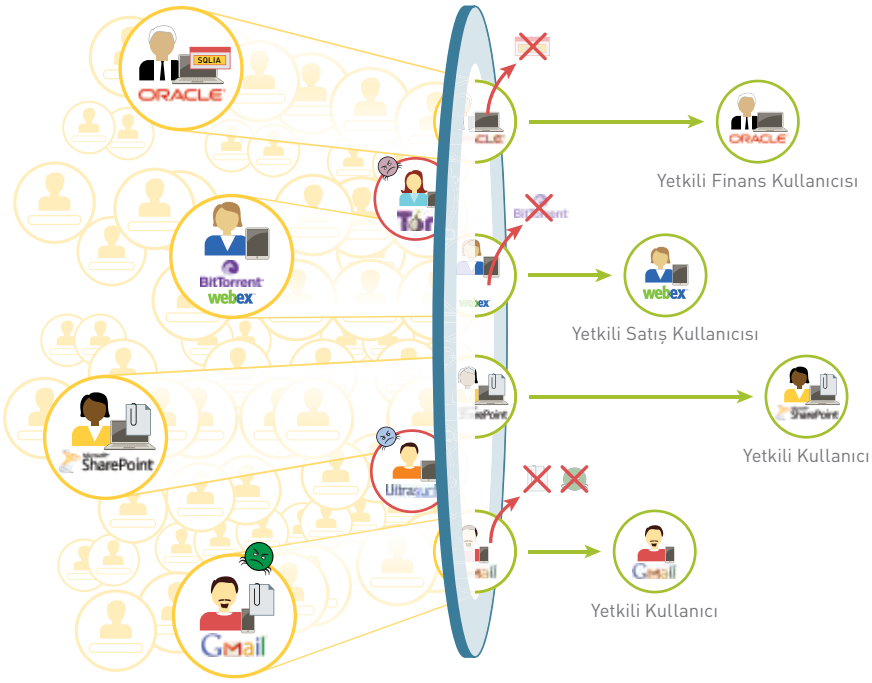
- **Portları değil uygulamaları belirlemek.** Kullanılan protokol, şifreleme veya tehdit önlemeyi atlatma taktiği ne olursa olsun uygulama kimliğini saptamak için güvenlik duvarına gelir gelmez trafiği sınıflandırın. Sonra bu uygulama kimliğini bütün güvenlik kararları için temel alın.
- **Uygulama kullanımını, konuma veya cihaza bakmaksızın, IP adresine değil, kullanıcı kimliğine bağlayın.** Konumları veya kullandıkları cihaz ne olursa olsun, bütün kullanıcıları kapsayan tutarlı güvenlik politikaları oluşturmak için kuruluşların dizin sunucularındaki veya diğer kullanıcı adres veritabanlarındaki kullanıcı ve grup bilgilerinden yararlanın.
- **Bilinen veya bilinmeyen tüm tehditlere önleyin.** Trafiği bilinen güvenlik açıkları, zararlı yazılımlar, casus yazılımlar, kötü amaçlı URL'ler açısından analiz edin ve otomatik olarak yüksek oranda hedeflenen ve daha önceden bilinmeyen kötü amaçlı yazılımlara karşı koruma sağlarken bilinen tehditleri de önleyin.
- **Politika yönetimini basitleştirin.** Kullanımı kolay grafiksel araçlarla, entegre politika düzenleyicisi ve cihaz gruplarıyla yönetimsel işleri azaltıp uygulamaları güvenli kılın.

Güvenli uygulama kullanım politikaları, hangi lokasyon söz konusu olursa olsun, güvenlik seviyenize ait büyük resminizi geliştirmenizi sağlar. İstenmeyen bir dizi uygulamayı dış katmanda engelleyip ardından izin verilen uygulamaları hem bilinen, hem bilinmeyen tehditler açısından inceleyerek tehdit olasılığını azaltabilirsiniz. Klasik veya sanal olsun veri merkezinde güvenli uygulama kullanımını etkinleştirmek, taşınan içeriğin tehditlerden ayıklanarak ve sanal altyapıların dinamik doğası gereği karşılaşılan güvenlik sorunları giderilerek veri merkezi uygulamalarının yalnızca yetkili kullanıcılar tarafından kullanılması anlamına gelir. Kuruluşunuzun şubeleri ve uzak kullanıcılar, şirket merkez lokasyonunda uygulanan güvenli uygulama kullanım politikalarının aynısı ile korunarak kurum çapında güvenlik politikalarında tutarlık sağlanır.



paloalto NETWORKS
the network security company™

UYGULAMALAR, KULLANICILAR VE İÇERİK – HEPSİ KONTROLÜNÜZ ALTINDA



İşinize Güç Katmak İçin Güvenli Uygulama Erişimi

Uygulamaların Palo Alto Networks yeni nesil güvenlik duvarıyla güçlü biçimde denetlenmesi, şirket ağı üzerinde çalışan ve sayısı hızla artan uygulamaların getirdiği güvenlik ve işle ilgili risklerden korunmanıza yardımcı olur. Uygulamaları hem yerel, hem mobil ve uzak kullanıcılar veya gruplar için etkinleştirip trafiği bilinen ve bilinmeyen tehditlere karşı koruduğunuzda, işletmeniz büyürken güvenlik resminizi de sağlamlaştırırsınız.

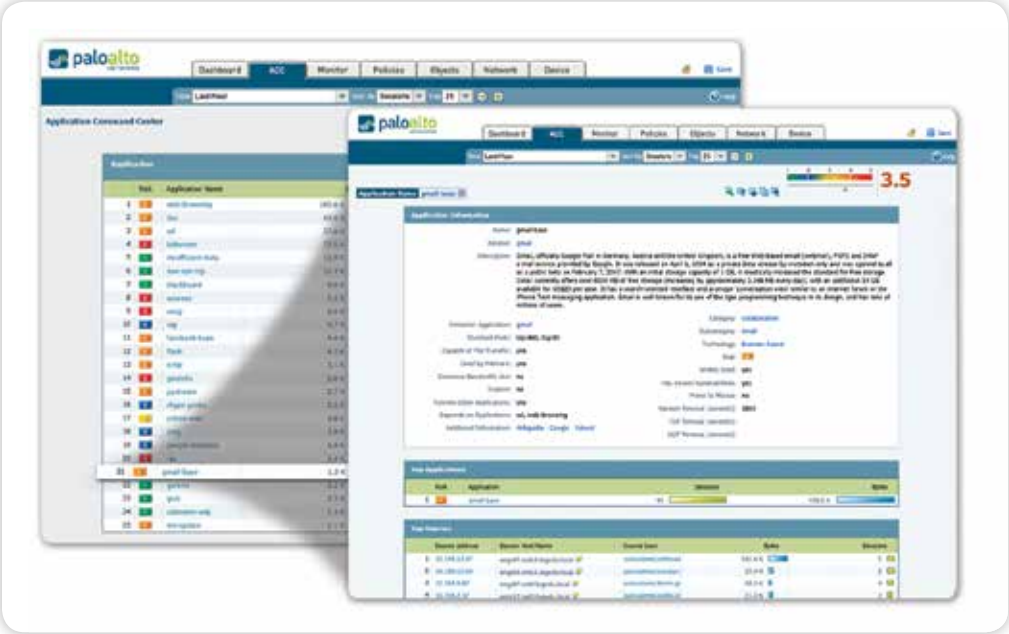
- **Tüm uygulamaları, her zaman, tüm portlarda sınıflandırma.** Trafik sınıflandırmasının hassas biçimde doğru olarak yapılması bütün güvenlik duvarlarının kalbini ve güvenlik politikalarının temelini oluşturur. Günümüzde artık uygulamalar, porttan porta atlayarak, SSL ve SSH kullanarak, port 80 üzerinden gizlice geçerek veya standart dışı portlar kullanarak port/protokol temelinde çalışan güvenlik duvarlarını kolaylıkla aşabilmektedir. App-ID, port, şifreleme (SSL veya SSH) ya da kullanılan tehdit önleme atlatma tekniği ne olursa olsun, şirket ağınızda dolaşan uygulamanın gerçek kimliğini saptamak için trafik akışı güvenlik duvarına gelir gelmez trafiğe birden fazla sınıflandırma mekanizması uygulayarak klasik güvenlik duvarlarının en büyük hastalığı olan trafik sınıflandırması görünürlük sınırlamalarını giderir. Sadece port veya protokolleri değil ağınızın tümünde hangi uygulamaların kullandığı bilgisi, bütün güvenlik politikası kararlarınızın temelini oluşturur. Tipik olarak trafiğin küçük bir yüzdesi olmasına karşın yüksek risk potansiyeli taşıyan tanımlanmamış/tanınmayan uygulamalar otomatik olarak, politika denetimi ve incelemesinin, vaka sonrası incelemesinin, özel App-ID oluşturmanın veya Palo Alto Networks App-ID geliştirmesi için paket yakalamanın (packet capture) gibi metotların da dahil olduğu sistematik bir yönetim bütünü içinde kategorize edilir ve denetim altına alınır.

- **Politikalarla yalnızca IP adreslerini değil, kullanıcıları ve cihazları da tümleştirme.** Güvenlik politikalarını cihaza veya konuma bakmaksızın, uygulamayı ve kullanıcı kimliğini temel alarak oluşturma ve yönetme, ağınızı korumak için yalnızca port ve IP adresine güvenmekten çok daha etkin bir yoldur. Kurumsal kullanıcı dizin servisleri ile entegrasyon, herhangi bir uygulamaya erişimi olan Microsoft Windows, Mac OS X, Linux, Android veya iOS kullanıcısının kimliğini tespit etmenizi sağlar. Seyahat eden veya uzaktan çalışan kullanıcılar, yerel veya şirket ağında kullanılan aynı tutarlı politikalarla sorunsuz bir şekilde korunur. Kullanıcının uygulama kullanımının görünürlüğü ve denetimi, kullanıcı nereden veya nasıl erişim sağlarsa sağlasın, şirket iç ağınızda çalışan Oracle, BitTorrent veya Gmail ya da başka herhangi bir uygulamanın kullanımını güvenle sağlayabileceğiniz anlamına gelir.

- **Bilinen veya bilinmeyen tüm tehditlere karşı önlem alın.** Günümüzün modern ağlarını korumak için bilinen birçok güvenlik açıklarına, kötü amaçlı ve casus yazılımlara karşı önlem almanın yanı sıra hiç bilinmeyen ve hedeflenmiş (targeted) tehditleri de önlemeniz gerekir. Bu süreç, sadece bilinen ya da kurumsal çapta ihtiyaç duyulan belli başlı bazı uygulamalara izin verip geri kalan tüm uygulamaları reddederek ağ üzerinden gerçekleştirilen atakların etki alanını daraltarak başlar. Bundan sonra eşgüdümlü tehdit önleme izin verilen trafiğin tümü üzerinde, bilinen kötü amaçlı yazılım sitelerini, güvenlik açıklarını, virüsleri, casus ve kötü amaçlı yazılım DNS sorgulamalarını tek bir geçişle engelleyerek uygulanabilir. Bilinmeyen dosyalar 100'den fazla kötü amaçlı davranışı takip eden sanal bir kum torbası ortamında çalıştırılıp doğrudan gözlemlenerek özel ya da bilinmeyen kötü amaçlı yazılımlar aktif biçimde analiz edilir ve belirlenir. Yeni kötü amaçlı yazılımlar bulunduğunda, bulaşmaya neden olan dosya ve ilgili kötü amaçlı trafik için otomatik olarak imza oluşturulur ve size gönderilir. Bütün tehdit önleme analizleri tüm uygulama ve protokol içeriğini kullandığından şifrelenmiş tünellerde, sıkıştırılmış içerikte veya standart dışı bağlantı portlardan akarak saklanmayı deneseler bile tüm tehditlerin daima yakalanmasını sağlar.

Dağıtım ve Yönetim Esnekliği

Uygulamaları güvenli kılma işlevi, bu amaca uygun üretilmiş bir donanım platformunda veya sanal bir ortamda kullanılabilir. Birden fazla Palo Alto Networks güvenlik duvarını, ister donanım olarak isterseniz de sanal sistem olarak devreye aldığınızda, üzerlerinden akan trafiği gözlemek, üzerilerinde güvenlik politikası yaratmak, rapor oluşturmak ve içerik güncellemelerini merkezi bir konumdan görebilmek olanağı sağlayan, opsiyonel bir merkezi bir yönetim ürünü olan Panorama'yı kullanabilirsiniz.



Uygulama Görünürlüğü: Uygulama hareketlerini açık, kolay okunur bir biçimde görüntüleyin. Uygulama, işlevleri ve bunları kimin kullandığı hakkında daha fazla bilgi için filtreler ekleyip kaldırın

Güvenli Uygulama Kullanımını Etkinleştirme: Kapsamlı bir Yaklaşım

Güvenli uygulama, ağınızın tamamen güvenli bir hale gelmesi ve işinizin büyümesi için ağ üzerindeki uygulamalar hakkında ayrıntılı bilgi sahibi olmakla başlayan, kullanıcının kim olduğu, platform veya konumu ne olursa olsun uygulamada, eğer varsa, ne içerik bulunduğu bilgisiyle devam eden kapsamlı bir yaklaşımı gerektirir. Ağ üzerindeki etkinliklerle ilgili daha fazla bilgiyle donandığınıza uygulama öğelerini, kullanıcıları ve işinize ilişkin içeriği temel alan daha anlamlı güvenlik ilkeleri oluşturabilirsiniz. Kullanıcının konumu, platformu ve politkanın nerede (dış katmanda, klasik veya sanal veri merkezinde, şubede veya uzak kullanıcıda) uygulandığı, politikanın oluşturulmasını çok az etkiler ya da hiç etkisi olmaz. Bundan sonra artık bütün uygulamaları, kullanıcıları ve içerikleri güvenle etkinleştirebilirsiniz.

Eksiksiz Bilgi Daha Sıkı Güvenlik Politikaları Anlamına Gelir

Tecrübe göstermektedir ki, ağınız hakkında eksiksiz bilgi sahibi olmak daha güçlü güvenlik politikaları uygulamanızı sağlamaktadır. Örneğin, sadece port bilgisini temel alan daha geniş bir trafik profiline kıyasla ağınızda tam olarak hangi uygulamaların etkin olduğunu bilmek, yöneticilerinizin istenmeyen uygulamaları engellerken yalnızca işinizle ilgili uygulamalara izin vermesine olanak sağlar. Sadece IP adresinin değil kullanıcının da kim olduğunu bilmek, politikaların atanmasında daha seçici olmanızı sağlayan başka bir ölçüttür.

- Yöneticileriniz, güçlü grafiksel görüntüleme araçlarını kullanarak uygulama etkinliklerinin, olası güvenlik sorunlarının daha eksiksiz bir resmini görebilir ve ilkesel kararları verirken bilgiye dayanırlar. Uygulamalar sürekli olarak sınıflandırılır ve durumları değiştikçe, bilgileri kullanımı kolay, web tabanlı arabirimde görüntüleyen grafik özetler dinamik olarak güncellenir.
- Yeni ya da tanınmayan uygulamalar, tek bir tıklatmayla uygulamanın açıklamasının, davranış özelliklerinin ve kimin kullandığının görüntülenmesiyle hızla araştırılabilir.
- URL kategorileri, tehditler ve veri düzenleriyle ilgili ek görüntüler, ağ üzerindeki trafiğin tam bir özet resmini verir.
- Genel olarak her ağın küçük bir yüzdesini oluşturmasına karşın büyük risk taşıyan bilinmeyen uygulamalar, henüz tanınmayan ticari yazılımlar, dahili uygulamalar ya da tehdit olup olmadıklarının belirlenmesi için analiz edilmek üzere sınıflandırılır.

Uygulamaları Etkinleştirme ve Riskleri Azaltma

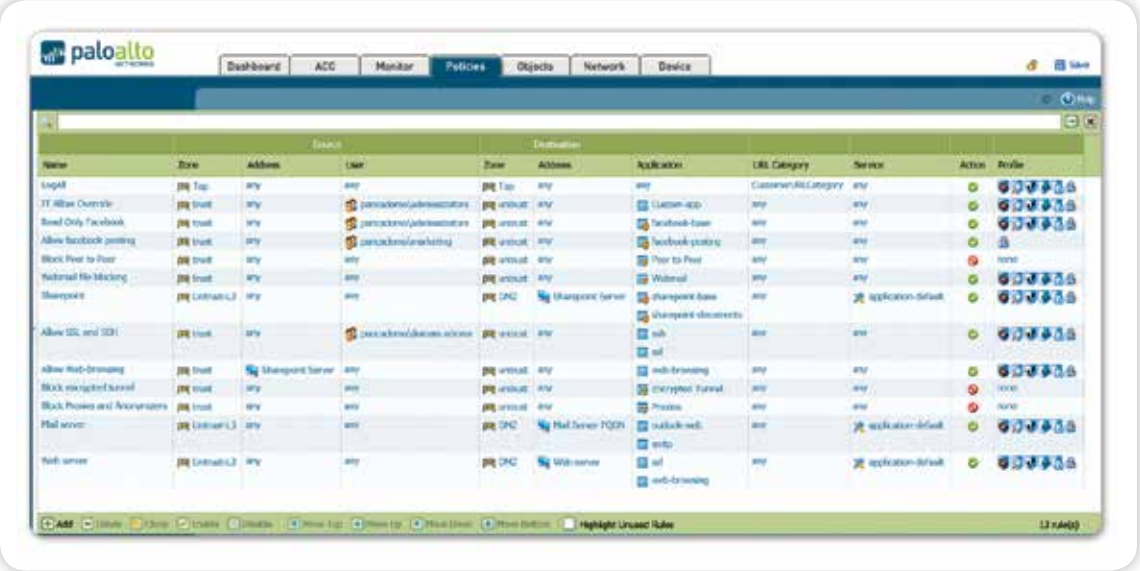
Güvenli uygulama etkinleştirmesi, tüm uygulamaların reddedilmesi (ki iş yapamaz hale gelmenize sebep olur) ile yüksek risk taşıyan tüm uygulamalara izin verilmesi (ki sınırsız sayıda riski de beraberinde getirir), aralarında bir orta nokta bulmak için arasında uygulama/uygulama işlevi, kullanıcılar, gruplar ve içeriğin olduğu politika karar kriterlerini kullanır.

Güvenli uygulama kullanım politikaları, şubelerin, mobil ve uzak kullanıcıların olduğu birimlerde tüm trafiğin belirlenmesine odaklanır ve sonra kullanıcı kimliğini esas alarak seçici biçimde trafiğe izin verir ve ardından tehditler açısından trafiği tarar. Politikalara şunlar örnek gösterilebilir:

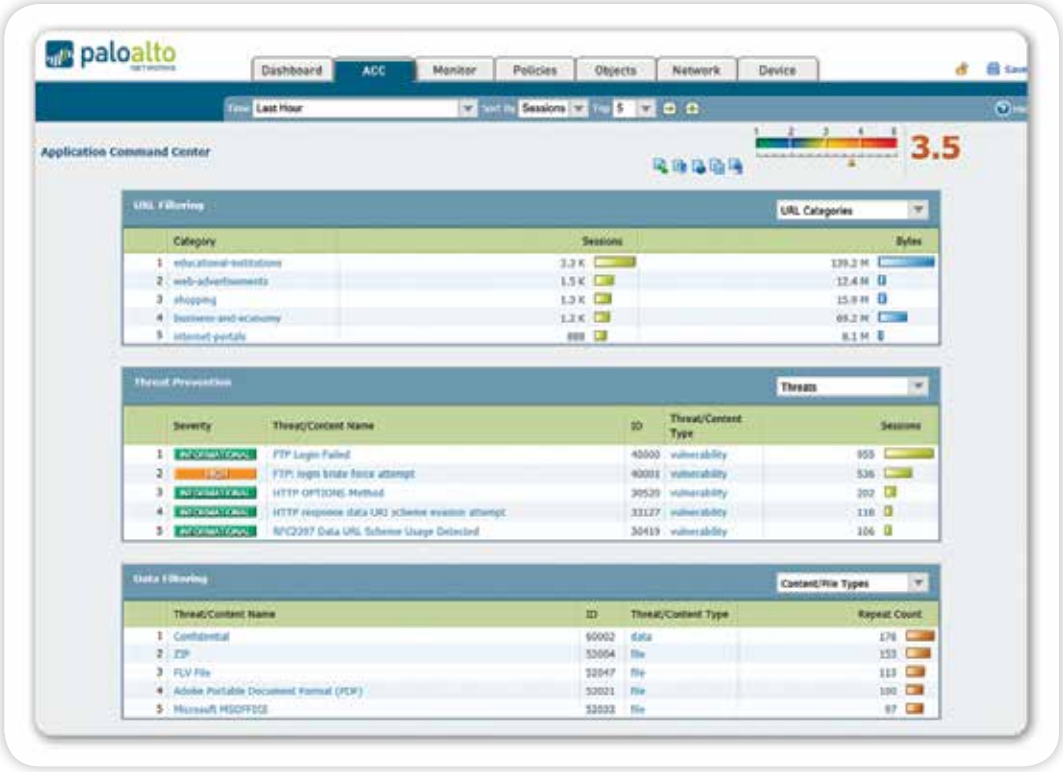
- Web posta ve anlık ileti kullanımını birkaç çeşidiyle sınırlama, SSL kullananların şifresini çözme, trafiği güvenlik açıkları açısından inceleme ve analiz edilip imza geliştirilmesi için bilinmeyen dosyaları WildFire sistemine gönderme.
- Akış halindeki ortam uygulamalarına ve web sitelerine izin verme fakat VoIP uygulamalarına olan etkilerini engellemek için QoS ve kötü amaçlı yazılım korumasını uygulama ve ağı koruma.
- Kullanıcıların "taramasına" izin verip Facebook oyunlarını ve sosyal eklentileri engelleyerek ve yalnızca pazarlama amacıyla Facebook'a yüklemeye izin vererek Facebook'u kontrol altında tutma. Tüm Facebook trafiğini kötü amaçlı yazılım ve güvenlik açıkları için tarama.
- İşle ilgili olmadığı açık olan web sitelerine erişimi engellerken işle ilgili web sitelerine olan trafiğe ve taramaya izin vererek web'de dolaşmayı denetim altında tutma, özelleştirilmiş blok sayfalar üzerinden tartışmalı sitelere olan erişimi "yönlendirme".
- GlobalProtect sayesinde aynı politikaları bütün kullanıcılara, konumlara, mobil veya uzak kullanıcılara şeffaf bir biçimde uygulayarak tutarlı bir güvenlik oluşturma.
- İş ve güvenlik riski oluşturan uygulama trafiğini azaltmak için dolaylı olarak "şunlar dışındaki hepsini reddet" veya "P2P ve arkadan dolaşan ya da belirli ülkelerden gelen trafik gibi istenmeyen uygulamaları doğrudan engelleme" stratejisini kullanma.

Klasik, sanal ya da her ikisinin bileşimi veri merkezindeki etkinleştirme örnekleri, uygulamaların onaylanmasına, zararlı uygulamalara ve verilerin korunmasına odaklanmıştır.

- Oracle tabanlı kredi kartı numarası deposunu kendi güvenlik alanında yalıtın, finans gruplarına erişimi denetleyin, trafiğin standart portlardan yapılmasını zorlayın ve uygulama güvenlik açıkları için trafiği inceleyin.
- Standart portlar üzerinden sabit uzaktan yönetim uygulamalarını (ör., SSH, RDP Telnet) kullanarak yalnızca BT grubunun veri merkezine erişmesine izin verin.
- Microsoft SharePoint Yönetimi'nin yalnızca kendi yönetici ekibiniz tarafından kullanılmasına, diğer tüm kullanıcıların da Microsoft SharePoint Belgelerine erişmesine izin verin.



Entegre Politika Düzenleyicisi: Alışıldık görünüm ve kullanım, uygulamaları, kullanıcıları ve içeriği denetleyen politikaların hızla oluşturulabilmesini ve dağıtılmasını olanaklı kılar.



İçerik ve Tehdit Görünürlüğü: URL, tehdit ve dosya/veri aktarım etkinliklerini açık, kolay okunur bir biçimde görüntüleyin. Tek tek öğeler hakkında daha fazla bilgi almak için filtreler ekleyin, kaldırın.

Etkinleştirilen Uygulamaları Koruma

Güvenli uygulama etkinleştirmesi, belirli uygulamaların kullanılmasına izin verilmesi ve sonra bilinen güvenlik açıklarının, bilinen ya da bilinmeyen kötü amaçlı ve casus yazılımların engellenmesi için belirli politikaların uygulanması, dosya veya veri aktarımıyla web'de dolaşma etkinliklerinin denetlenmesi anlamına gelir. Port atlama ve tünel açma gibi sıklıkla görülen tehdit önlemeyi atlatma taktikleri, App-ID decode'ları tarafından uygulama ve protokol çözümleme yöntemleri kullanılarak yürütülen tehdit önleme politikaları ile önlenir. Buna karşılık, tehdit önleme için silo tabanlı bir yaklaşım sergileyen UTM çözümlerinde, her işlevin, güvenlik duvarının, IPS, AV, URL filtrelemesi vs. gibi güvenlik motorlarının hepsinin gördükleri içeriği paylaşmadan trafiği taraması, bunları, atlatma davranışlarına daha elverişli bir hale getirmektedir.

- **Bilinen Tehditleri Engelleyin: IPS ve Ağ Virüs Koruması/Casus Yazılım Önleme.** Tekdüzen bir imza biçemi ve akış-temelli tarama motoru, ağınızın geniş bir tehdit yelpazesinden korunmasını sağlar. Yetkisiz erişim önleme sistemi (IPS), ağ ve uygulama katmanı güvenlik açıklarının, bellek taşmalarının, DoS saldırılarının ve port taramalarının engellenmesini kapsar. Virüs koruması/ Casus yazılım önleme koruması milyonlarca kötü amaçlı yazılım çeşidini engellediği gibi kötü yazılımların ürettiği komuta kontrol trafiğini, PDF virüslerini ve sıkıştırılmış dosyalarda veya web trafiğinde (sıkıştırılmış HTTP/HTTPS) gizlenen kötü amaçlı yazılımları da engeller. Tüm uygulamalardaki ve bağlantı noktalarındaki politika tabanlı SSL şifre çözme, sizi SSL şifreli uygulamaların içinden geçen kötü amaçlı yazılımlara karşı korur.
- **Bilinmeyen, Hedeflenen Kötücül Yazılımları Engelleyin: Wildfire™.** Bilinmeyen veya hedeflenen kötücül yazılımlar, bilinmeyen dosyaları doğrudan bulut tabanlı sanal korumalı bir ortamda çalıştırıp bunların davranışlarını gözlemleyen WildFire tarafından belirlenip analiz edilir. WildFire 100'den fazla kötü amaçlı davranışı izler ve sonuçları hemen uyarı biçiminde yöneticiye gönderir. İsteğe bağlı bir WildFire aboneliği geliştirilmiş koruma, log tutma ve raporlama özelliklerini sunar. Abone olarak, dünyanın her hangi bir yerinde kötücül bir yazılımın bulunmasından itibaren bir saat içinde söz konusu yazılımın yayılması durdurularak sizi etkilemeden önce korunmaya alınırsınız. Abone olarak entegre WildFire log kaydı ve raporlaması ile bulut analizi amacıyla örneklerin WildFire'a gönderilmesi için API erişimi de kazanırsınız.

- **BotNet'lerin Parçası Olmuş Bilgisayarları Belirleyin.** App-ID, bilinmeyen trafik dahil olmak üzere bütün uygulamaları, tüm portlarda sınıflandırır; ki bu da çoğu zaman ağınızdaki gariplikleri ve tehditleri ortaya çıkarır. Davranış esaslı botnet raporu bilinmeyen trafiği, şüpheli DNS ve URL sorgulamalarını ve muhtemelen kötücül yazılımlar tarafından etkilenen cihazları ortaya çıkarmak için olağan dışı ağ davranışlarını ilişkilendirir. Sonuçlar, olası botnet üyesi olarak araştırılması gereken bir etkilenen bilgisayarlar listesi biçiminde görüntülenir.
- **İzinsiz Dosya ve Veri Aktarımını Engelleyin.** Veri filtreleme özellikleri yöneticilerinizin, izinsiz dosya ve veri aktarımı ile ilişkili riskleri azaltacak politikaları uygulamalarını sağlar. Dosya aktarımları, aktarıma izin verilip verilmeyeceğinin belirlenebilmesi için, yalnızca dosya uzantısına bakmak yerine, dosyanın içine bakılmasıyla denetlenebilir. Genel olarak Internet'ten indirilen dosyalarda bulunan yürütülebilir dosyalar engellenerek ağınız, görülmeyen kötücül yazılımın yayılmasından korunabilir. Veri filtreleme özellikleri, gizlilik derecesi olan veri düzenlerini (kredi kartı veya vatandaşlık numaralarının yanı sıra özel düzenleri) algılayabilir ve denetleyebilir.
- **Web'de Dolaşmayı Denetleyin.** Tamamen tümleştirilmiş, özelleştirilebilir URL filtreleme motoru yöneticilerinizin, uygulama görünürlüğü ve denetim politikalarını tamamlayan ayrıntılı web taraması ilkelerini uygulamalarına olanak sağladığı gibi kuruluşunuzu bütün hukuki, mevzuat gereksinimleri ve iş üretkenliği risklerine karşı da korur. Buna ilaveten, SSL şifre çözme, QoS veya diğer kural esasları için daha fazla denetim ayrıntısı sağlayan politikalara yönelik olarak URL kategorilerinden de yararlanabilinir.

Yönetim Devamlılığı ve Analiz

En iyi güvenlik uygulamaları, söz konusu ister tek bir cihaz ister yüzlercesi olsun, yöneticilerinizin güvenlik duvarını etkileşimli olarak yönetmeleriyle araştıran, analiz eden ve güvenlik olaylarını raporlayan tepkisel bir yönetim biçimi arasında denge kurmalarının gerektiğini göstermektedir.

- **Yönetim:** Bütün Palo Alto Networks platformları komut satırı arabirimiyle (CLI) veya tam özellikli tarayıcı tabanlı bir arabirimle yönetilebilir. Büyük ölçekli dağıtımlar için Panorama lisansı alınabilir ve şablon kullanımı ve paylaşılan politikalar gibi özellikleri kullanılarak yerel politika esnekliği ihtiyacıyla merkezileştirilmiş genel denetimi dengelemenizi sağlayan bir merkezi yönetim çözümü olarak Panorama kullanılabilir. SNMP gibi standartları temel alan araçlar ile REST tabanlı API'lar için sağlanan ilave destek, üçüncü taraf yönetim araçlarıyla tümleştirebilme olanağı verir. İster cihazın ister Panorama'nın web arabirimini kullanıyor olun, arabirim görünümü ve kullanımı aynı olduğundan, birinden diğerine geçerken öğrenme eğrisi söz konusu olmaz. Yöneticileriniz, eşitleme sorunlarıyla uğraşmadan her hangi bir sırada değişiklik yapmak için sağlanan arabirimlerden birini kullanabilir. Rol tabanlı yönetim tüm yönetim ortamlarında desteklendiğinden özellikleri ve işlevleri belirli kişilere atayabilmenize olanak sağlar.
- **Raporlama:** Önceden tanımlanan raporlar, ihtiyaca göre, olduğu gibi, özelleştirilmiş biçimde veya birlikte gruplanarak tek bir rapor şeklinde kullanılabilir. Bütün raporlar CSV veya PDF biçiminde dışa aktarılabilir ve zamanlanarak yürütülebilir ve e-postayla gönderilebilir.
- **Log tutma:** Gerçek zamanlı log kaydı filtrelemesi, ağınızdaki her oturumun hızla olay sonrası incelemesinin yapılmasını kolaylaştırır. Log kaydı filtresi sonuçları CSV dosyasına dışa aktarılabilir veya çevrimdışı arşivleme veya başka analizler için syslog sunucusuna gönderilebilir.

Amaca Uygun Üretilmiş Donanım veya Sanal Platformlar

Palo Alto Networks, kurumların uzak şubeleri için tasarlanmış PA-200 modelinden, yüksek hızlı veri merkezleri için tasarlanmış PA-5060 modeline kadar tam bir amaca uygun üretilmiş donanım platformları dizisi sunmaktadır. Platform mimarisi tek geçişli yazılım motorunu temel alır ve istenilen performansı göstermesi için ağ iletişimi, güvenlik, tehdit önleme ve yönetim unsurları için işleve özel işlem işlemciler kullanır. Donanım platformlarında verilen aynı güvenlik duvarı işlevselliği, çevre veya uzak ofis güvenlik duvarlarına uygulanan aynı ilkeleri kullanarak sanal ve bulut tabanlı bilgisayar ortamlarını güvenli hale getirmenizi sağlayan VM-Series sanal güvenlik duvarında da kullanılabilir.

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