Yeni Nesil Güvenlik Duvarım (NGFW) Var, Neden Ayrıca Bir Web Uygulaması Güvenlik Duvarına (WAF) İhtiyacım Olmalı?

Müşteriler ilk olarak, "Yeni Nesil Güvenlik Duvarım (NGFW) Var, Neden Ayrıca Bir Web Uygulaması Güvenlik Duvarına (WAF) İhtiyacım Olmalı?" sorusuna yanıt aramaktadır. Bundan 4-5 yıl önce ortaya atılan bu sorunun cevabı, zaman içerisinde kurumların ihtiyaçlarıyla birlikte kendiliğinden ortadan kalkmıştır. Bir Web Uygulaması Güvenlik Duvarının sunabileceği katma değere odaklanarak her iki çözüm arasındaki farkı açıklayalım:

Web uygulaması nedir?

Öncelikle, bir Web Uygulamasının tam olarak ne olduğunu bilmek önemlidir. Web uygulaması, uzak bir sunucuda depolanan ve bir tarayıcı arayüzü aracılığıyla İnternet üzerinden gönderilen bir uygulama programıdır. Web'in ilk günlerinde web siteleri, kullanıcıyla etkileşimi ciddi şekilde sınırlanmış statik sayfalardan oluşuyordu. Ancak son 30 yıldır, web sunucuları, sunucu tarafındaki özel komut dosyalarıyla iletişime izin verdiği için bu sınırlar kaldırıldı. Kullanıcıyla uygulama arasındaki etkileşim, kuruluşların e-ticaret, web tabanlı e-posta, internet bankacılığı, bloglar, web forumları ve iş faaliyetlerini desteklemek için özel platformlar gibi pek çok olanağa dönüşmüş ve hem kurumsal hem de kişisel hayatlarımız tümüyle uygulama dünyasına dönüşmüştür. Tüm bu web uygulamaları, web tarayıcısı ile web sunucusu arasındaki bağlantı için protokol olarak HTTP(S) kullanır.

Web uygulamaları, zengin arayüz parçaları, kapsamlı framework'ler ve karmaşık üçüncü taraf kitaplıkları için HTML5, Java, JavaScript, PHP, Ruby, Python ve / veya ASP.NET gibi dillere ve komut dosyalarıyla birlikte çok daha karmaşık hale geldi. Asıl önemlisi bu web uygulamalarının, arkadaki veritabanlarına bağlanan kritik iş araçları olmasıdır. Bu veritabanları, şirket verileri, kart sahibi verileri gibi hassas verilerin tutulduğu alanlardır ve bu nedenle yüksek ölçüde korunmalıdır. Öte yandan web uygulamaları, açık olmaları ve internet üzerinden kolayca erişilebilmeleri nedeniyle siber suçlular için oldukça ilgi çekici hedeflerdir. Bugün, güvenlik açısından yaşadığımız zorluğun tümüyle ortaya çıktığı oyun alanı tam da burasıdır. Artık, "Neden bir WAF'a ihtiyacım var?" sorusu hepimizin sıklıkla duyduğu hikayelerin bir parçasıdır.

Yeni Nesil Güvenlik Duvarı (NGFW) Nedir?

Geleneksel bir güvenlik duvarı, paket filtreleme, ağ ve bağlantı noktası adresi çevirileri (NAT) ve VPN'ler gibi işlevlerle sınırlıdır. Kararlarını bağlantı noktaları, protokoller ve IP adreslerine göre verir. Günümüzde güvenlik politikalarını bu kadar esnek olmayan ve şeffaf olmayan bir şekilde uygulamak artık ne pratik ne de güvenlik açısından yeterlidir. Yeni bir yaklaşıma ihtiyaç vardır ve NGFW'ler, güvenlik politikalarına daha fazla bağlam ekleyerek bu yaklaşımı sağlamaktalar. Bu yeni sistemler, daha etkili güvenlik kararları vermek amacıyla konum, kimlik, zaman vb. bilgileri akıllı bir şekilde kullanmak üzere tasarlanmıştır.

EXCLUSIVE NETWORKS

Yeni Nesil Güvenlik Duvarları, URL filtreleme, virüsten koruma / kötü amaçlı yazılımdan koruma, Saldırı Önleme Sistemleri (IPS) ve daha fazlası gibi özellikler ekleyerek kendilerini geleneksel güvenlik duvarlarından ayırır. Birkaç farklı nokta çözümü kullanmak yerine, bir NGFW, giderek karmaşıklaşan bir bilgi işlem dünyasında güvenlik politikalarının uygulanmasının etkinliğini büyük ölçüde basitleştirir ve geliştirir.

Web Uygulaması Güvenlik Duvarı (WAF) Nedir?

Web uygulaması güvenlik duvarları, web sunucularını ve barındırılan web uygulamalarını HTTP(S) aracılığıyla uygulama katmanındaki saldırılara ve ağ katmanındaki volumetric saldırılara karşı korur. WAF'lar, ağ trafiğinizin bir bölümünü, özellikle internete yönelik genel web uygulamalarına karşı korumak için tasarlanmıştır. WAF'lar ayrıca bu zayıflıklar için sanal yama sağlayarak potansiyel olarak güvenli olmayan kodlama açıklıklarını telafi edebilir. Bir WAF, müşterinin web uygulamalarının tasarımına göre özelleştirilebilir. Çoğu zaman, WAF'ler bir Application Delivery Controller (ADC) üzerinde In-line olarak kurulur.

Açık Web Uygulama Güvenliği Projesi (OWASP Top 10), CWE /SANS En Tehlikeli İlk 25 Yazılım Hatası, Web Application Security Consortium (WASC), Threat Classification v2.0 ve Cross Reference View; gibi regüle edilmiş global web tehditleri referanslarına genel bir bakış sağlar. Tüm bu potansiyel tehditler, özelleştirilmiş Web Uygulaması Güvenlik Duvarı teknolojisine olan vihtiyacı haklı çıkarır. Özetle, WAF konumlandırmak, kodu güvenli hale getirmeye çalışmanın, PCI DSS, HIPAA, Basel II ve SOX vb. regülasyonlara uyumluluğunu sağlayabilmenin en öncelikli yoludur.

Bir F5 WAF'ın katma değeri nedir?

Bir web uygulamasının özel olarak oluşturulmuş karakteri ve trafik düzeni eşleşmesine dayanan korumalardan kaynaklanan false pozitif veya performans eşikleri gerçek bir sorun haline gelebilir. NGFW veya İzinsiz Giriş Önleme Sistemi (IPS) katmanı, bu tür sorunları azaltmak için Web uygulaması koruma imzalarının çoğunu varsayılan olarak devre dışı bırakır. Bununla birlikte, NGFW ve IPS ürünleri yalnızca temel bir imza seti sağlar ve bir WAF'ın daha gelişmiş özellikleriyle donatılmamıştır.

WAF ise temel olarak Policy-Based (“Positive”) security ve Signature-based (“Negative”) security özelliklerini destekler. F5 WAF, gerçek zamanlı(realtime) olarak politika oluşturabilir; otomatik self-learning ve policy oluşturma özelliğine sahiptir. Bu sayede vulnerabilitileri keşfetme özelliği sağlar.

F5 Networks WAF, web protokolleri ve dil bilgisi ile trafik kod çözme ve normalleştirme gerçekleştirmek için özel motorlara sahiptir. Daha gelişmiş SSL / TLS şifre çözme / boşaltma yetenekleriyle birleştiğinde WAF, kapsamlı web saldırısı imza veritabanının etkinliğini artırır.

F5 Networks, web saldırısı imza veri tabanının yanı sıra, web uygulamasına kullanıcı girişi üzerinde derin ve ayrıntılı bir kontrol için URL, Parametre, Cookie ve Form Koruma yetenekleri sunar. Bir politika öğrenme motoru tarafından desteklenen WAF güvenlik politikalarının uygulanması. Bu politika öğrenme motoru, istemcilerden gelen HTTP (S) isteklerini ve web uygulamalarının cevaplarını dinler. Bu şekilde, zorlanacak veya beyaz listeye eklenecek URL'lerin, parametrelerin ve web saldırı imzalarının bir haritası oluşturulur.

Ayrıca F5 WAF, siteler arası talep sahteciliğini önlemek için URL şifreleme, web sayfalarına kod yerleştirme, tanımlama bilgisi imzalama ve özel hata sayfaları gibi tekniklerle web uygulamaları tarafından gönderilen yanıtların değiştirilmesi yoluyla web uygulamalarınızı korur.

Son bir fark yaratan F5 WAF, bir web uygulamasının normal iş akışını bozabilecek kötü amaçlı etkinlikleri tespit etmek için kullanıcı oturumlarını izler ve ayrıca gelişmiş bot önleme ve DDoS önleme algılama motorlarına sahiptir. İsteğe bağlı olarak F5 Networks WAF, Tek Oturum Açma, Çok faktörlü kimlik doğrulama (MFA) ve / veya web uygulamalarının ön kimlik doğrulaması gibi gelişmiş kimlik doğrulama hizmetleri de sağlayabilir.

EXCLUSIVE NETWORKS