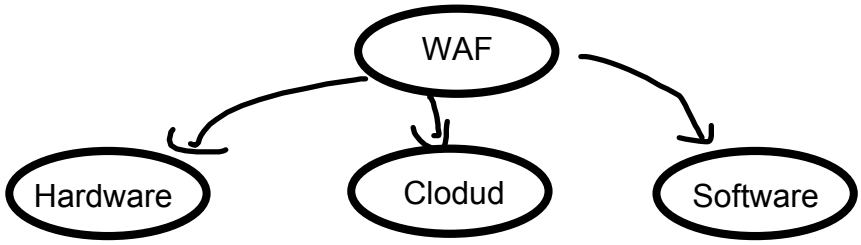
WAF(Web Application Firewall):

Bugün sizlere Web Application Firewall ile ilgili en sade bilgiyi aktarmaya çalışacağım, öncelikle şunu belirtmek isterim ki, bu web sitesinin amacı karşıda ki kişiye bilmesi gereken bilgiyi, en doğru ve sade şekilde aktarmak, fakat Anlatım biçimi veya eksik bilgi verme durumları söz konusu olabilir, Unutulmaması gerekiyor ki bu yeni bir proje ve gelişim sürecinde, Zamanla bu sorunlar çözülecek ve konu başlıkları derinlemesine işleneceği zaman dilimi gelecektir keza "Bu web sitesinin Amacı nedir" adlı yazımı kesinlikle okumanızı öneriyorum, Şimdi geçelim.

HTTP protokolü var olduğu yıldan bugüne, kullanım biçimi fazlasıyla değişti. tabi ki de bunun etkisi internetin bu kadar gelişmesi ve word wide web'in hayatımıza girmesi büyük etken, insanların bu kadar kolay internete erişebiliyor oluşu ve bu etkenler. HTTP protokolü üzerinden bazı güvenlik sorunlarınıda beraberinde getirdi. Bu güvenlik sorunlarını ise hiç anlamayan bir kişiye telaffüz etmem gerekirse, günlük hayatta girdiğimiz web siteleri üzerinden bize yapılan atak vektörü veya kullandığımız web sitesine yapılan atak vektörü diyebiliriz. İşte bu atak vektörleri üzerine hayatımızıa Web Application Firewall girdi, WAF dediğimiz bu teknoloji Normal Firewall ile karşılaştırılmaması gerekiyor, ikisinin arasındaki en sade anlatım biçimini ifade etmem gerekirse, Normal Firewall OSI 3 ve 4 katmanlarında çalışırken, WAF teknolojisi 7 katmanda çalışması. yani Normal firewall Ip ve Port tabanlı kontrol sağlarken, WAF teknolojisi Uygulama tabanlı kontrol sağlıyor, Çünkü web uygulaması üzerinden yapılan bu atak vektörü uygulama katmanını(application layer) ilgilendiren bir durum. bunun üzerine WAF nedir sorusuna yönelelim.

WAF Nedir:

WAF Teknolojisi, Web Uygulamasına gelen ve giden veri paketlerini izleyen,filtreleyen ve engelleyen bir güvenlik aracıdır diyebiliriz. Bu güvenlik aracı ise kendi içerisinde kullanım biçimi olarak 3'e ayrılıyor. bunlara aşağıda vermiş olduğum şemaya bakabiliriz.



Donanım Tabanlı WAF:

Sunucunun bulunduğu Local Area Network ağında, fiziksel olarak kurulan WAF türü diyebiliriz. Cihaz içinde yazılım yapılandırmalarını ve güncellemelerini destekleyen bir işletim sistemi ile çalışır.

Donanım Tabanlı WAF, Sunucuya yakınlığı nedeniyle bize vermiş olduğu en büyük avantajı Yüksek Hız ve Yüksek perfonmans kazandırması. web sitesine giden ve gelen veri paketlerini çok düşük gecikmeyle izler ve fitreler. ama tabi ki de her şeyin bir avantajı olduğu gibi dezavantajıda var. Donanım tabanlı WAF'lar, maliyet açısından çok pahalı. Kullanım yerlerini ise çok büyük firmalar haricinden pek rast gelmezsiniz.

Yazılım Tabanlı WAF:

Yazılım tabalı WAF, donanım yerine virtual machine üzerine kurulan WAF türü diyebiliriz. Donanım tabanlı WAF ile aynı şekilde çalışır fakat Perfonmansbakımından değişiklik gösterir. Web uygulamasına gelen giden paketlerin, izleme ve filtreleme süresini artırır. Donanım Tabanlı WAF türüne göre en büyük avantajı maliyet bakımından ucuz ve esnek olması. kullanım yerleri ise küçük ve orta ölçekli işletmeler diyebiliriz.

Bulut Tabanlı WAF:

Bulut Tabanlı WAF, Günümüz dünyasında yeni nesil olarak adlandırdığımız WAF türü diyebiliriz. Diğer WAF türlerinin aksine, WAF bileşenleri tamamen bulutta bulunur, bu sayede kullanıcının yerel veya bir sanal makineye herhangi yükleme işlemi yapmasına gerek kalmaz. Bulut Tabanlı WAF türünün bize vermiş olduğu en üyük avantaj Basitlik olmakla birlikte en büyük dezavantajı ise WAF'ın tamamen servis sağlayıcı tarafından yönetilmesi nedeniyle özelleştirmeye fazla yer olmamsıdır, tabi ki de bu anlatılanlara daha da vakıf olabilmek açısınıdan Cloud nasıl çalışır hakkında bilgimizin olması gerekiyor.

WAF NASIL ÇALIŞIR:

Aslında böyle soruların cevabını görsel üzerinden anlatırım fakat bu yazımda sözel olarak ilerleyeceğim. bu şekildede olaylara vakıf olacağınıza inanıyorum. WAF, White list(Beyaz liste) veya Black list(kara liste) üzerine kurulan, gelen paketler sunucuya varmadan önce durduran ve ilgili yapılandırmaya göre filtreleyen bir teknoloji diyebiliriz.

WAF'lar tarafında önlenene saldırıların bazıları:

burada maddeler halinde verilen atak vektörlerini, sırasıyla başka bir yazıda ele alacağım. O yüzden burada açıklama gereği duymadım.

****Enjeksiyon Saldırıları***

****HTTP Ddos(Flood) saldırıları***

****Dizin geçiş saldırıları(Directory Traversal)***

****Server Side Reqeust Forgery***

****Clickjacking***

Tabi ki de WAF'ların özelliklerinide konuşmak gerekiyor fakat WAF ile ilgili bu kadar bilgi şimdilik yeterli olduğunu düşünüyorum. Özellikle ileride Teknik bilgi açısındıan ModSecurity ile ilgili bir yazı yazarsam, ayrıntılı olarak WAF yazısı yazacağımı bildirmek isterim. Şimdilik bu kadar.

e-mail

berathanakcakaya@gmail.com

linkedin

https://www.linkedin.com/in/berathan-akcakaya/