ÜNİTESİ **:** Satın Alma Müdürlüğü

SAYI **:** 2023 / 15610

KONU **:** Load Balancer Alım İşi.

SON BAŞVURU TARİHİ **:** 1 Kasım 2023 Çarşamba saat 16:00

Türkiye Futbol Federasyonu tarafından; Gayrettepe TT Datacenter'da konuşlandırılmak üzere Load Balancer + Waf özellikli cihaz alımı için ihale düzenlenecektir. İhaleye ilişkin teknik bilgiler aşağıdadır.

İstekliler, tekliflerini kapalı zarf usulü "Hasan Doğan Milli Takımlar Kamp ve Eğitim Tesisleri Çayağzı Köyü Riva Beykoz/İstanbul" adresinde mukim Türkiye Futbol Federasyonu Satın Alma Müdürlüğüne 01.11.2023 Çarşamba saat 16:00'a kadar teslim edebilirler.

İstekliler, hazırladıkları teklife esas evraklarını iki ayrı zarfa koyacaklardır. Bu zarflar, dış zarf ve iç zarf diye anılmaktadır. Teklif mektubu ve geçici şartname kapalı ve mühürlü bir iç zarfa konarak, diğer belgeler ile birlikte dış zarf içinde verilecektir.

DIŞ ZARF:

- Tebligat adresini gösterir belge (gerçek kişilerde ikametgâh belgesi, tüzel kişilerde adrese ilişkin ticaret sicil gazetesi),
- Şirkete ait son Ticaret Sicil Gazetesi ve noter tasdikli imza sirküleri veya ihaleye katılmaya yetkililere ait vekaletname,
- Son 3 ay içerisinde alınmış ticaret odası faaliyet belgesi,
- Noter tasdikli vergi levhası fotokopisi,
- Referans Dosyası,
- Sosyal Güvenlik Kurumu'ndan borcu olmadığına ilişkin teklif tarihinden önce en fazla 10 gün içinde alınmış ıslak imzalı belge,
- İlgili Vergi Dairesi'nden borcu olmadığına ilişkin teklif tarihinden önce en fazla 10 gün içinde alınmış ıslak imzalı belge,

İÇ ZARF:

- Teklif mektubu, (firma yetkilisi tarafından imzalanmış ve kaşelenmiş olacaktır.)
- Geçici Teminat (Teklif bedelinin % 5'i değerinin karşılığı olan teminat tutarında ve teklif tarihinden itibaren 30 gün süreli hükümetçe yetkili kılınan veya milli bir banka tarafından düzenlenmiş geçerli teminat mektubu veya aynı tutara karşılık gelecek nakdi tutarın TFF'ye ödendiğine ilişkin makbuzun teklif dosyasında yer alması gerekmektedir)

Teklifler kapalı ve mühürlü bir iç zarfa konarak, diğer belgeler ile birlikte dış zarf içinde verilecektir. Dış zarf üzerinde sadece "**LOAD BALANCER ALIM İŞİ**" ibaresi yer alacaktır.

İstekli ihaleyi kazanması halinde, teklif bedelinin % 10'u tutarında kati teminat sunacaktır. Kati teminat süresizdir, hükümetçe yetkili kılınan veya milli bir banka tarafından düzenlenmeli ve her halükarda işin tümüyle istenen nitelikte tamamlanmasından sonra iade edilir.

Teklif zarflarının tesliminden sonra İstekli teklifinden vazgeçemez veya değiştirilmesini öneremez. TFF, 2886 sayılı Devlet İhale Kanunu ve 4734 sayılı Kamu İhale Kanunu'na tabi olmayıp, 5894 sayılı yasa ile özel hukuka tabi, özerk bir tüzel kişiliktir. Bu bağlamda, işbu ihale süreci tümüyle özel hukuk hükümlerine tabi olup, TFF verilen teklifleri dilediğince değerlendirme ve İSTEKLİLER ile sözleşme yapıp yapmama konusunda tamamıyla serbesttir. TFF, teklifleri kendi belirleyeceği kıstaslar kapsamında değerlendirme ve serbestçe seçim yapma hakkına sahiptir ve ihaleye katılmak isteyenlerin **tekliflerini e-ihale sistemine dahil etme hakkı bulunduğunu da saklı tutar.**

TFF ihale aşaması, satın almanın katileştiğinin İSTEKLİ'ye tebliğinden sonra veya sözleşme akdedilmesine ilişkin süreç sırasında İSTEKLİ'ye bildirimde bulunmak kaydıyla tek taraflı ve tazminatsız olarak ihaleden veya sözleşme akdinden sarfınazar edebilir.

Teknik Şartname

Aşağıda özellikleri belirtilen sistem; 1 (bir) adet Sunucu Yük Dengeleme, Web Uygulama Güvenlik çözümleri tek bir platformda yazılım ve donanım bütünü (appliance) olarak satın alınacaktır.

1. Cihaz Genel Özellikleri

1.1. Cihaz yedek çalışabilen 2 adet AC güç kaynağını desteklemelidir.

1.2. Cihaz üzerinde aynı anda farklı versiyon yazılım imajı kurulabilmelidir. Sistemin default olarak yüklü imajlardan hangisi ile açılacağı belirlenebilmelidir. Ayrıca istenmesi durumunda sistemin açılışı sırasında konsoldan bağlanarak, yüklü imajlardan hangisi ile boot edileceği de

seçilebilmelidir. Bu sayede versiyon yükseltme sonrası problem yaşanması durumunda bir önceki versiyon ile sistemi açabilmek mümkün olmalıdır.

1.3. Cihaz USB portuna bağlanacak harici disk üzerinden boot edilebilmelidir. Gerekmesi durumunda sisteme yeni imaj kurulumu boot edilen harici disk üzerinden yapılabilmelidir.

1.4. Cihazların her biri üzerinde 128 GB RAM olacaktır.

1.4.1. En az 95 Gbps Layer 4 throughput.

1.4.2. En az 60 Gbps Layer 7 throughput.

1.4.3. En az 1,000,000 Layer 4 CPS – Connection per second (saniyede yeni oturum açabilme kapasitesi).

1.4.4. En az 18,000,000 L4 HTTP RPS - request per second (saniyede işlenebilecek HTTP istek sayısı).

1.4.5. En az 2,500,000 Layer 7 RPS - request per second (saniyede işlenebilecek L7 istek sayısı).

1.4.6. En az 75.000.000 L4 eşzamanlı oturum sayısı (concurrent connection).

1.4.7. En az 35 Gbps SSL throughput.

1.4.8. En az 30.000 (ECDHE P-256-RSA 2K) SSL TPS – transaction per second.

1.4.9. En az 35 Gbps sıkıştırma (compression) throughput sağlamalıdır.

1.5. Cihazın üzerinde SSL şifreleme için özel kartı bulunmalıdır.

1.6. Web arayüzü üzerinden raporlama ve istatistiksel veri izleme yapılabilmelidir.

1.7. Farklı yetkilere sahip kullanıcı tanımlamaları yapılabilmelidir.

1.8. Cihaz konfigürasyonu harici bir ortama yedeklenebilmeli ve gerektiğinde yeniden yüklenebilmelidir.

1.9. İşletim sistemi yükseltme veya önceki sürüme dönme işlemleri web arayüzünden yapılabilmelidir.

1.10. Sistem üzerinde yönetim için ayrı bir ağ bağlantısı olmalı ve out-of-band yönetim yapılabilmelidir. Yönetim için sisteme verilen IP adresine özel ayrı bir default gateway (default route) tanımlanabilmelidir.

1.11. Sistemin donanım tanı (hardware diagnostic) desteği bulunmalıdır. Bunun için gerekli yazılım bileşenleri sistem üzerinde yüklü gelmelidir. Son kullanıcı, donanım tanı işlemini kendisi sistem üzerinde yapabilmelidir. İstendiği durumda donanım tanı bilgileri online olarak üretici firma web sitesine yüklenerek, daha detaylı olarak gerçek zamanlı analiz ve tanı kullanınıcının kendisi tarafından yapılabilmelidir.

1.12. Cihazlarda, SNMP v1, SNMP v2 ve SNMP v3 desteği bulunacaktır.

1.13. Cihazlar, SNMP trap ile üzerindeki up/down olayını, başka bir yönetim sistemine iletmesi sağlanacaktır.

1.14. Cihazlar, SNMP tabanlı sistemler ile entegre edilecektir. Yüklenici, cihazla etkileşim için SNMP MIB dosyalarını sağlayacaktır.

1.15. Cihazlarda, canlı performans, erişilebilirlik ve istatistikî bilgiler grafik ara yüzünden takip edilmesi sağlanacaktır.

1.16. Sistem üzerinde tanımlanan web servisleri için arka taraftaki sunucudan cevap dönüş süresi (server latency), uygulama sayfasının yükleme süresi (Application Page Load Time), erişilen URL listesi, erişen kullanıcıların IP adresleri, saniyedeki işlem miktarı (Transaction Per Second), istek için ve cevap için (request ve response) ayrı olarak bandgenişliği kullanımı (throughput), hangi ülkeden erişim sağlandığı, kullanıcı isteğine dönen cevap kodu (response code), kullanıcı tarayıcısı ve istek içindeki HTTP metodu bilgileri kullanıcı oturumları bazında (unique user session) izlenip geriye yönelik görsel olarak raporlanabilmelidir. Raporlar belirlenen email adresine otomatik ve düzenli olarak PDF veya CSV formatında email ile gönderilebilmelidir. İzlenen ve raporlanan parametreler ile ilgili belirlenen kriterlerin aşılması durumunda sistem otomatik olarak bilgilendirme mesajları (E-mail, syslog ya da SNMP trap olarak) gönderebilmelidir. Bu fonksiyonların sağlanması için gerekli tüm lisanslar sistem üzerinde yüklü gelmelidir. Eğer sistem bu fonksiyonları kendi üzerinde sağlayamıyorsa, gereken ek donanım/yazılım ve lisanslar teklife dahil edilmelidir.

1.17. Cihazlarda, syslog desteği bulunacaktır. Trafiğin log amaçlı uzak birden fazla syslog sunucusuna iletimi mümkün olmalıdır. Aynı zamanda syslog sunucu pool tanımlanarak logların gönderimi sırasında log sunucularından birisinin devre dışı kalması durumunda kesintisiz uzak sisteme loglamaya devam edebilmelidir.

1.18. Sistem yüksel-hızlı uzak loglama (high-speed remote logging) desteklemelidir. Ek özelleştirmeye gerek olmadan, log gönderilecek hedef olarak ArcSight, Splunk ve uzak syslog dış sistemleri tanımlanabilmelidir.

2. Cihazın Yük Dengeleyici Özellikleri

2.1. Cihaz, HTTP trafiği için GZIP ve DEFLATE compression yapabilme özelliğine sahip olmalıdır.

2.2. Yük dengelemeyle beraber sistem üzerinde SSL sonlandırma özelliği olacaktır. SSL Decryption (SSL şifresini çözme), cihaz üzerinde yapılıp, istemci - sistem arası HTTPS, sistem - sunucu arası, HTTP protokolü ile konuşacak şekilde konfigüre edilebilmeli ve farklı SSL profilleri tanımlanabilmelidir.

2.3. Sistemin IPV6 desteği olacaktır. Bu özellik için lisans gerekiyorsa teklife dahil edilmelidir.

2.4. Değerleri ayarlanabilir sunucu durum takip, izleme (monitoring) ara yüzü bulunmalıdır. Timeout(zaman aşım süresi) ve interval değerleri tanımlanabilme özelliği olmalıdır.

2.5. Sunuculara veya sunucu guruplarına ayrı ayrı ve birden fazla izleme tanımı yapılabilmelidır.

2.6. Sunucuların izlenmesi ICMP, TCP, HTTP, HTTPS, FTP gibi protokolleri kullanarak yapılabilmelidir.

2.7. Round Robin, Ratio, Least Connection yük dengeleme algoritmalarına sahip olacaktır.

2.8. Sistem, bütün sunucuların göçmesi veya aktif üyelik bilgilerine bakarak yönlendirme (redirection) yapmalıdır.

2.9. Sistem, tüm HTTP isteklerini veya belli bağlantıları, otomatik olarak HTTPS ’e çevirebilme özelliği olacaktır.

2.10. İstemcinin aynı sunucuda çalışmasını sağlayan Cookie persistence, Destination address affinity, source address persistence, özelliklerini desteklemelidir.

2.11. L4 ve L7 özelliklerine göre trafiği yönetebilme özelliği olmalıdır.

2.12. Sistemin, L2 mode switching (anahtarlama), L3 mode routing (yönlendirme) özelliği olmalıdır.

2.13. HTTP isteğindeki herhangi bir bilgiye göre (URL, Domain, Cookie, IP gibi) anahtarlama (Content Switching) yapacaktır. Bağlantıdaki herhangi bir bilgiye bakarak, sunucu kümelerinde yük dengeleme yapmalıdır.

2.14. Sistem, DMZ ve intranetteki farklı alt ağlarda (subnet) bulunan sunucular için yük dengelemesi yapabilecek şekilde konumlandırılabilmelidir. DMZ ile lokal ağ arasında networksel izolasyon sağlayabilmelidir.

2.15. Sistemin 802.3ad link aggregation (bağlantı arabirimi birleştirme) desteklemelidir. Bu özellik için lisans gerekiyorsa teklife dahil edilmelidir Cihazlarda, Packet Filtering ve Access Control List özellikleri bulunacaktır. Cihazlar, cihaza giren ve cihazdan çıkan trafiği, IP adresi ve port seviyesinde kontrol edebilmelidir.

2.16. Sistem, Network Address/Port Translation yapabilmelidir.

2.17. Sistemin her ethernet portunda “VLAN” ve “Tagged VLAN” teknolojileri desteklemelidir.

2.18. Cihazlarda, scriptlerle sunucunun sağlık kontrolü (Health Check) yapılabilmeli, up/down anlama süresi ayarlama özelliği olacaktır.

2.19. Cihazların konfigürasyon yedeği, cihazdan harici ortama export (yedekleme) ve import (geri yükleme) özelliği olacaktır

2.20. Yük paylaşımı yapılan sunucuların günlük kayıtlarında, kullanıcıların IP adreslerinin görülmesini ve loglanmasını mümkün kılmalıdır.

2.21. Yüklenici, harici bir gözlemleme sisteminin cihazlardan bilgi alabilmesi için gerekli XML API’leri sağlayacaktır.

2.22. Sistem Spanning Tree Protokolünü (STP) desteklemelidir.

2.23. Sistemin 802.1p desteği olmalıdır. QoS için, diğer çevre ağ bileşenleri (switch, router vb.) tarafından set edilen 802.1p önceliklendirme taglarını anlayabilmeli ve uyumlu çalışmalıdır.

3. Uygulama Güvenlik Duvarı Özellikleri

3.1. Uygulama Güvenlik Duvarı, Policy-Based (“Positive”) security ve Signature-based (“Negative”) security özelliklerini desteklemeli, imza güncellemesi manuel ya da otomatik yapılabilmelidir.

3.2. Uygulama Güvenlik Duvarı, katmanlı (layered) güvenlik politikaları oluşturup kullanmaya imkân vermelidir. Ana politika içerisinde farklı uygulamaların ortak olarak kullanacağı güvenlik politika kuralları oluşturulup, sonrasında her uygulama için sadece o uygulamaya özel güvenlik politikası oluşturup her biri aynı ana politikaya bağlanabilmelidir.

3.3. Uygulama Güvenlik Duvarı, host-tabanlı (Host-based) güvenlik politikası uygulamaya (enforcement) imkân sağlayabilmelidir. Aynı sanal sunucuya gelen farklı uygulamalara ait trafik için (örneğin tek bir virtual IP üzerinden www.abc.com, partners.abc.com, app1.abc.com uygulamalarına ait trafiğin geçmesi) farklı enforcement uygulanabilmelidir. Bir uygulama için uygulama güvenlik duvarı güvenlik politikası şeffaf (transparent) modda çalışırken bir diğeri için engelleme (blocking) modunda çalışabilmelidir.

3.4. Uygulama Güvenlik Duvarı, arka tarafta uygulama sunucuları üzerinde kullanılan işletim sistemi, veri tabanı, programlama dili, web sunucusu gibi teknolojileri otomatik olarak tespit edebilmeli ve bunlara uygun olarak koruma özellikleri önerebilmelidir.

3.5. Uygulama Güvenlik Duvarı, HTTP trafiğinin dışında SMTP ve FTP servisleri için güvenlik kuralları oluşturabilmelidir. FTP servisi için protokol uyumluluk kontrolü yapabilmeli, bruteforce ataklara karşı koruyabilmeli, FTP komutları için whitelist oluşturabilmeli. Komut uzunluklarını limitleyebilmeli SMTP servisi için greylist oluşturup spam atağına karşı koruyabilmeli, SMTP komutlarının kontrolü için black list oluşturabilmeli directory harvesting atakları azaltmalıdır.

3.6. Uygulama Güvenlik Duvarı, Layer 7 DoS, Brute Force, Cross-site scripting, Cross Site Request Forgery, SQL injection, Parameter tampering, Sensitive information leakage, Session high-jacking, Buffer overflows, Cookie manipulation, encoding attacks, Broken access control, Forceful browsing, Hidden fields manipulation, Request smuggling, XML bombs/DoS ataklarına karşı koruma sağlayabilmelidir.

3.7. Uygulama Güvenlik Duvarı, HTML5 CORS (Cross-Origin Resource Sharing) özelliği ile uyumlu şekilde Cross Domain Request Enforcement uygulayabilmelidir.

3.8. Uygulama Güvenlik Duvarının, WebSocket desteği olmalıdır. WebSocket kullanan uygulamalarının trafiğini WebSocket protokol özelinde parse edebilmeli, protokol özelinde güvenlik kontrolleri uygulayabilmeli ve WebSocket uygulamaları özelinde şu atak tiplerine karşı koruma sağlayabilmelidir: server stack abuse, session riding or CSRF, information leakage, XSS, SQL injection, comman shell injection, server exploits, cache poisioning, buffer overflow, exhausted server socket resources.

3.9. Uygulama Güvenlik Duvarı, WebSocket uygulamaları için listelenen ataklara karşı koruma için belirli kontrolleri sağlayabilmelidir. İstek içerisinde belli başlıkları zorunlu tutabilmelidir. Beyaz listede (whitelist) yer almayan orijinden gelen erişim isteklerini tespit edip engelleyebilmelidir. ws:// ve wss:// adresleri için oturum açmayı (login sessions) zorlayabilmelidir. Herbir WebSocket metin mesaj içeriğini, atak imza veritabanını kullanarak analiz edebilmeli ve bir atak deseni bulduğunda WebSocket bağlantısını kapatıp güvenlik kaydı oluşturabilmelidir. WebSocket mesajları için RFC uyumluluk, geçersiz meta-karakter ve boş (null) karakter kontrolleri yapabilmelidir. WebSocket kullanan uygulamalarda, istemci metin mesajları için maskelemeyi mecbur tutarak yanlış içeriğin belleğe kaydedilmesini (cache poisioning) engelleyebilmelidir. Mesaj boyutu ve mesaj çerçeve boyutunu (frame size) kısıtlayabilmelidir. Eğer mesaj JSON formatında ise içeriği doğrulayabilmelidir. WebSocket mesajlarının gönderim süresini ve mesajlar arasındaki süreyi kısıtlayabilmelidir.

3.10. Uygulama Güvenlik Duvarı, pozitif yaklaşım ile korudukları web sunucuların çalışma mantığını sayfalarda girilen input değerlerinin ne olması gerektiğini öğrenebilmeli ve bunlar haricindeki erişimlere izin vermemelidir. Gerektiğinde bu değerler elle müdahale edilerek değiştirilebilmelidir. Öğrenilen sayfaların değişmesi durumunda tekrar öğrenilmesi mümkün olmalıdır.

3.11. Uygulama Güvenlik Duvarı, realtime dinamik olarak policy oluşturabilmeli, otomatik self-learning ve policy oluşturma özelliğine sahip olmalıdır. Bu sayede zafiyetleri keşfetme ve hızlı kurulum özelliklerine sahip olmalıdır. Çift yönlü çalışıp data ve protocol seviyesinde güvenlik sağlamalıdır.

3.12. Uygulama Güvenlik Duvarı, web uygulaması kapsamındaki, kullanıcı kimlik doğrulama sayfaları ve formlarını (login pages and forms) ek konfigürasyona gerek olmadan otomatik olarak tespit edebilmelidir. Tespit edilen sayfa ve formlar için şifre ataklarına karşı koruma mekanizmalarını (brute force attack protection) otomatik olarak devreye alabilmelidir.

3.13. Uygulama Güvenlik Duvarı, izin verilen ya da engellenen HTTP metotlarını, her URL özelinde ayrı şekilde konfigüre edebilmeye imkân vermelidir.

3.14. Uygulama Güvenlik Duvarı, uygulamayı öğrenebilme özelliğine sahip olmalıdır.

3.15. Uygulama Güvenlik Duvarı, Kredi Kartı ve vatandaşlık numarası gibi hassas dataları algılayabilmeli ve belirli politikalar takibinde bu bilgilerin anons edilmesini önleyebilmelidir.

3.16. Uygulama Güvenlik Duvarı, uygulamadan dönen hata kodlarını ve hata sayfalarının görüntülenmesini engellemelidir.

3.17. Uygulama Güvenlik Duvarı, engellenen bir erişime ait kayıtları detaylı bir şekilde saklamalıdır. Bu kayıt en az tarih, saat, kaynak IP, hedef IP, hedef URL ve engelleme sebebi bilgilerini içermelidir.

3.18. Uygulama Güvenlik Duvarı, istenildiği takdirde üzerinden geçen HTTP isteklerini ve yanıtlarını ayrıntılı olarak loglayabilmelidir. Her bir istek veya yanıta bağımsız ve ayrı ID’ler atayarak takip kolaylığı sağlamalıdır.

3.19. Uygulama Güvenlik Duvarı, erişim ve güvenlik kayıtlarını birden fazla destinasyona eş zamanlı olarak gönderebilmelidir. Eş zamanlı olarak hem kendi yerel diski üzerinde kayıt tutabilirken hem de uzak kayıt sunucusuna (gerekirse eş zamanlı birden fazla uzak sunucuya) kayıtları gönderebilmelidir.

3.20. Uygulama Güvenlik Duvarı, üçüncü parti uygulama ve cihazlarla entegre olarak çalışabilmelidir, örneğin Splunk, White Hat ve ArcSight.

3.21. Uygulama Güvenlik Duvarı, SSL içinden gelen saldırıları yakalayabilmelidir. Cihazın kendi üzerinde içerik filtreleme yapabilmesi tercih nedenidir. Yazılımcı tarafından unutulan klasörler, yedek dosyalar ve istemci tarafında istenmeyen HTTP isteği reddedilebilmelidir.

3.22. Uygulama Güvenlik Duvarı ile ilgili admin yetkileri sadece belli bir user rolünde olmalıdır.

3.23. Uygulama Güvenlik Duvarı, üzerinde ayrıntılı rapor alınabilmelidir. Application Firewall'a yönelik raporlar, audit raporları alınabilmesi tercih nedenidir, rapor formatı PDF olmalıdır. Raporlar Schedule edilebilmelidir. Email ile gönderilebilmelidir.

3.24. Uygulama Güvenlik Duvarı, zafiyet taraması sonucunda tespit edilen açıklardan, otomatik olarak giderilmesi durumunda uygulama ile ilgili sorun oluşturabileceklerini ayrı bir sayfada listeleyebilmeli ve bunların elle giderilmesi için ne yapılması gerektiği konusunda ek bilgi sağlayabilmelidir.

3.25. Uygulama Güvenlik Duvarı, XML firewall özelliği olmalı, aşağıdaki fonksiyonlara sahip olmalıdır: WSDL Method Filtering, XML content inspection/validation, XML Denial of Service (XdoS) Recursive Expansion Attack, SQL injection via XML (Xpath) prevention, XML attachment security SOAP message validation, Schema validation, Request rate limiting.

3.26. Uygulama Güvenlik Duvarı, XML uygulamalarını ve web servislerini koruyabilmeli, XML formatını doğrulayabilmeli (validation of XML format), uygulamaya ait XML şema dosyaları ya da WSDL dokümanlarını kullanarak ilgili trafiğin bunlara uygunluk kontrolünü yapabilmelidir. Hassas XML verisini maskeleyebilmelidir. SOAP (Simple Object Access Protocol) mesajlarının istenilen kısımlarını şifreleme özelliği sunmalıdır. Dijital imza kullanarak SOAP mesajlarının istenilen kısımlarını imzalayabilmeli ve doğrulayabilmelidir.

3.27. Uygulama Güvenlik Duvarının Web Scraping koruma özelliği olmalıdır; Rate limiting, heuristics ve algorithms özellikleri ile uygulama hakkında bilgi alanın botnet olup olmadığını ayırt edebilmelidir.

3.28. Uygulama Güvenlik Duvarı, davranışsal analiz yapabilmeli (behavioural analysis) ve bu analiz sonucunda, uygulama seviyesinde gerçekleşen DDoS ataklarını otomatik olarak tespit edip koruma mekanizmalarını işletebilmelidir. Davranışsal analiz kapsamında, mouse ve klavye aktivitesi tespiti, mouse lokasyon takibi ile mouse'un bir noktadan bir noktaya gidiş süresinin ölçümü, klavye üzerinde yukarı ve aşağı tuş aktivitelerinin takibi ve süre ölçümlemesi, farklı klavye aktiviteleri arasındaki varyans ölçümlemesinin yapılması, bir oturumda uygulamanın farklı sayfalarına erişimler arasında geçen süre bilgilerinin ölçümlemesi gibi işlemler sistem tarafından yapılabilmelidir.

3.29. Uygulama Güvenlik Duvarı, DoS koruması kapsamında bot ataklarını tespit edebilmeli, gerçek tarayıcılar veya bot tarafından oluşturulan otomatik istekleri ayırt edebilmelidir. İstenildiği durumda, bot tarafından gönderildiği tespit edilen istekleri gönderen oturum için, ek olarak Captcha aktive edilebilmelidir.

3.30. Uygulama Güvenlik Duvarı, uygulama seviyesinde (L7) DoS atakları, deneme yanılma ile yapılan şifre atakların (brute force) ve oturum gasp ataklarını (session hijacking), cihaz kimliği (Device ID-Fingerprint) bilgisini kullanarak tespit edebilmelidir. Aynı şekilde analiz raporlarında da cihaz kimlik bilgisine göre filtreleme yapılabilmelidir.

3.31. Uygulama Güvenlik Duvarı, kullanıcının doğrulanması ve sunucu gecikmelerini izleyebilmeli ve değişimleri tespit ederek DoS/DDoS ataklarını anlayabilmelidir.

3.32. Uygulama Güvenlik Duvarı, DoS atağı tespit ettiğinde otomatik olarak atak sırasındaki trafiğin kopyasını (TCP dump) alabilmelidir. Bu trafik kopyasını kaydetme özelliği SSL trafiği için de çalışabilmelidir. Ayrıca yakalanan (captured) trafik kaydı, otomatik olarak dış bir sisteme gönderilebilmelidir.

3.33. Uygulama Güvenlik Duvarı, güvenlik kurallarını XML formatında export ederek audit ve off-line olarak programatik değişiklik için kullanabilme özelliğine sahip olmalıdır.

3.34. Uygulama Güvenlik Duvarının REST API desteği olmalıdır ve bu sayede sisteme bağlanmadan, program ve kod ile dışarıdan güvenlik politikası detayını görme ve güvenlik politikası üzerinde değişiklik yapmaya imkân verebilmelidir.