Web Application Firewall (WAF) Teknik Şartnamesi

Genel İstek ve Özellikler

- Teklif edilecek cihazın lisansı 1 yıl olacaktır.
- Teklifi sunan firma, WAF ürününün kurulum ve konfigürasyonunu sağlayacaktır.
- Teklif sunan firma, WAF ürününün lisans süresi boyunca bakım ve destek hizmeti verecektir.
- Teklif verecek firmaların sektörde en az 5 (beş) yıldır faaliyet göstermesi, İstanbul'da yerleşik ofisi ve bu ofiste çalışan en az 3 (üç) yıl deneyime sahip güvenlik destek uzmanı bulunduracaktır. Güvenlik destek uzmanı firmanın teklif edeceği WAF ürününün güncel sertifikasına sahip olmalıdır ve belgelendirilmelidir.
- Firma tarafından, Ticaret Üniversitesi personeli 3 kişiye WAF ürününün eğitim, işletme, bakım, kurulum, idame ve yönetim konularının eğitimi verilecektir. Üreticinin uluslararası yetkili eğitim merkezlerinde kullanılan "üretici firmanın standart sertifikalı yöneticilik/uzmanlık eğitimi" resmi eğitim materyalleri söz konusu eğitimler sırasında kullanılacaktır. Eğitim sadece teorik anlatımlardan ibaret olmamalı, uygulamalı olarak verilmeli, örnek projelerle desteklenmelidir. Eğitim yazılımlarda kullanılan tüm terimleri, komutları, menüleri, menülerdeki ekranları ve bir ekrandaki her işlevi detaylı olarak açıklamalı, ne işe yaradıklarını, hangi durumlarda ve nasıl kullanılmaları gerektiğini içermelidir. Eğitim sonunda katılımcılara, eğitim sonunda elde ettikleri yetkinlik ile ilgili hak ettikleri belgeler (katılım belgesi veya sertifika) verilecektir. Kullanıcılar verilen eğitimden memnun kalmaz veya eğitim sırasında aksaklık çıktığından eğitimden gerekli verim alınamaz veya eğitim süresi tüm içeriği anlatmaya yetmez ise, eğitimler İdare'nin uygun göreceği şekilde tekrarlanacaktır.

1. Kurulum Gereklilikleri

1.1. VMware ESX/ESXi/Fusion/Workstation/Player, Citrix Xenserver, Oracle VirtualBox, Microsoft Hyper-V sanallaştırma desteklemelidir.

1.2. WAF çözümü, 200 Mbps throughput, HTTP Transaction/Sec 30.000, SSL transaction/Sec. 12.000 değerlerini karşılamalıdır.

1.3. WAF çözümü Ipv4 ve Ipv6 trafiği desteklemelidir.

1.4. Teklif edilecek WAF çözümü, full reverse proxy modu desteklemelidir. Bu sayede tüm trafik WAF üzerinden yönlendirilebilmelidir.

1.5. Teklif edilecek WAF çözümü, SSL offload desteklemelidir.

1.6. Teklif edilecek WAF çözümü, PKI bilgilerini depolamak ve şifreleme işlemleri için bir Network HSM entegrasyonunu desteklemelidir.

1.7. Teklif edilecek WAF çözümü, HTTP trafik verilerine erişmek için şifrelenmiş trafiğin şifresini çözebilmelidir.
   a- Kullanıcılar için sertifika tabanlı kimlik doğrulama desteği olmalıdır.
   b- Alternatif taşıma yöntemleri kullanılarak, istemci sertifikalarındaki içeriğin uygulamaya gönderilebilmesi desteklenmelidir.
   c- WAF ile uygulama sunucusu arasındaki trafik şifrelenebilmelidir.
   d- Gerekli olan/ istenen cipher suite seçilmesine izin vermelidir.

1.8. Teklif edilecek WAF çözümü, HTTPS desteklemeyen sadece HTTP destekleyen uygulamaları güvenli hale getirebilmek için, uygulama sunucusunda herhangi bir yapılandırmaya gerek duymadan kendisi sertifika yayınlayabilecek ve böylece istemci ile WAF arasındaki trafik HTTPS, WAF ile uygulama sunucusu arasındaki trafik ise HTTP olarak çalışabilecektir.

2. Güvenlik Gereklilikleri

2.1. Teklif edilecek WAF çözümü, pasif güvenlik politikalarıyla yalnızca algılama modunda çalışmayı destekleyecektir. Bu sayede politikalar aktif konuma getirilip engelleme moduna geçmeden, paylaşılan uygulamalar için güvenli şekilde testler yapılacaktır. Bu testleri yapabilmek için mod ayarları, URL, Query/FORM arametreleri, çerezler ya da header bazında güvenlik ayarları gibi granüler seviyede yapılabilecektir.

2.2. Teklif edilecek WAF çözümü, aşağıdaki engelleme yeteneklerini desteklemelidir
   a- Connection reset
   b- Custom error response page
   c- Request redirection
   d- Block (belli bir süreliğine kullanıcı IP adresini bloklama)

2.3. Teklif edilecek WAF çözümü, HTTP rewriting özelliğine sahip olmalıdır. Bu sayede request ve response header ekleme, silme, ve değiştirme yapılabilmeli, URL translate yapılabilmeli, istekteki URL yeniden yazılıp yeniden yönlendirilebilmeli ve yanıt gövdesi yeniden yazılabilmeli. Bu işlemler için syntax gibi regular expression öğeler bulunmalıdır.

2.4. Teklif edilecek WAF çözümü, sistem yöneticisinin her bir URL için HEAD, CONNECT, TRACE vb... gibi birçok erişimi kısıtlamasına imkan vermelidir.

2.5. Teklif edilecek WAF çözümü, isteğin farklı bölümleri için farklı kısıtlama politikaları uygulanmasına izin vermelidir. Bu kısıtlamalar, uygulama – URL – sorgu/FORM parametreleri- header- çerezler ve request rate düzeylerinde yapılabilmelidir.

2.6. Teklif edilecek WAF çözümü, isteklerde aşağdaki protokol tabanlı kısıtlamaları desteklemelidir ve bunlar her bir URL için ayrıca belirtilebilir olmalıdır.

a- HTTP method length
b- Request line length
c- URI length
d- Query string length
e- Protocol length
f- Header name, value, and number
g- Request body length
h- Cookie name, value and number
i- Parameter name, value and number
j- Maksimum uzunluk (her bir dosya için) ve upload edilen dosya sayısı (POST)

2.7. Teklif edilecek WAF çözümü, cloaking yeteneğine sahip olmalıdır. Bu sayede sunucunun gönderdiği yanıt gövdesi ve yanıt başlığında bulunabilecek sunucuya ait hassas bilgileri gizlemek amacıyla hata yanıtlarını perdeleyebilmelidir.

2.8. Teklif edilecek WAF çözümü, yanıt gövdesini analiz edebilmelidir. Bu sayede; yanıt kodundan bağımsız olarak daha sonra bulunabilecek hassas bilgileri bloklayabilmeli ya da perdeleyebilmelidir. Çözüm burada kullanılmak üzere, hazırda kredi kartları için şablon (pattern) bulundurmalı ve istenirse diğer şablonlar regular expression formatında oluşturulabilir. Bu işlem için bir regex builder aracının bulunması tercih sebebidir

2.9. Teklif edilecek WAF çözümü, gelen URL isteklerinde örtüşen regular expression değerlerine göre filtreleme yapılırken negatif güvenlik modelini desteklemelidir.

2.10. Teklif edilecek WAF çözümü, pozitif güvenlik modelini desteklemelidir. Böylece, bir çok güvenlik politika elementinde diğer tüm değerler bloklansa bile izinli listesine alınmış olan değerlere izin verilebilmesini sağlamalıdır.

a- FORM/query parametreleri için izin verilmiş değerler (izin verilen veri tipleri, liste vb.) listesi
b- URL ve parametrelerde bulunan izinli meta karakter/anahtar kelimeler listesi
c- Geçerli uygulama profili - izin verilen URL'ler ve her ikisi için ayrı güvenlik profillerine sahip her URL'nin parametreleri
d- Her bir URL için izin verilen HTTP metodları
e- Her bir URL için izin verilen içerik tipi (Content Types)
f- İzin upload edilebilecek dosya uzantıları

2.11. Teklif edilecek WAF çözümü, form tampering işleminden korumak için alanları salt okunur olarak işaretleyebilmelidir.

2.12. Teklif edilecek WAF çözümü, OWASP top 10 listesinde belirtilen ataklara karşı koruma sağlamalıdır. Örn. SQL Injection, Cross Site Scripting, CSRF, Insecure Direct Object Reference vb...

2.13. Teklif edilecek WAF çözümü, parametrenin birden fazla instance a bölündüğü durumlarda trafiği analiz edebilmeli ve güvenliğinin sağlayabilmelidir

2.14. Teklif edilecek WAF çözümü, hıza dayalı (rate based) atak koruması sağlamalıdır.
- a- Erişim kontrollerine karşı Brute Force ataklar
- b- Uygulamanın herhangi bir kısmına yönelik Brute Force ataklarını (aynı kaynak için tekrarlanan istekler) engelleyebilecektir.
- c- Atak yapanı bloklayabilecek ya da yavaşlatabilecektir.
- d- Oturum yönetimine yapılan brute force atakları algılayabilecektir. (tek bir IP adresi ya da bir IP adres aralığından açılan fazla sayıda oturum gibi)

2.15. Teklif edilecek WAF çözümü, Session token koruması sağlamalıdır, örn. Çerezler
- a- İstemcinin değiştirmesini engellemek için çerezlerin imzalanması
- b- İçeriğin gizlenmesi için çerezlerin şifrelenmesi
- c- Cookie Replay ataklarının engellenmesi
- d- Belirli çerezlerin güvenlik kontrollerinden hariç bırakılması

2.16. Teklif edilecek WAF çözümü, gizli FORM alanlarının belirtilmesine ve tespit edilmesine izin vermelidir böylece alanları istemci tarafından değiştirilmeye karşı korumalıdır.

2.17. Teklif edilecek WAF çözümü, benzersiz URL'ler oluşturarak, bağlantıları oturuma özgü hale getirerek ve yönlendirme denetimlerini kullanarak CSRF saldırılarına karşı güvenlik önlemleri alabilmelidir.

2.18. Teklif edilecek WAF çözümü, upload edilen dosyalar için antivirüs ve anti malware taraması yapabilmelidir.

2.19. Teklif edilecek WAF çözümü, IP tabanlı olarak izinli/yasaklı listesi oluşturulmasına izin vermelidir.

2.20. Teklif edilecek WAF çözümü, gömülü Uygulama DDOS koruması içermelidir. Bu özellik için ek lisans gerekmemelidir.

3. Yönetimsel Gereklilikler

3.1. Teklif edilecek WAF çözümü, bir imza veri tabanı ile birlikte gelmelidir ve WAF'ın kural veri tabanı için en son imzaları manuel müdahale olmaksızın belirli periyodlarda otomatik olarak alması mümkün olmalıdır.

3.2. Teklif edilecek WAF çözümü, web saldırılarının, erişim trafiğinin ve sistem yöneticilerinin yaptığı işlemlerin kapsamlı bir şekilde günlüğe kaydedilmesini (loglanmasını) sağlamalıdır.

a- Yaygın olarak kullanılan log formatları desteklenmelidir. Örn. Common, W3C extended, NCSA extended vb.
b- Loglar syslog ve FTP sunucularına gönderilebilmelidir.
c- Istenen güvenlik politika ihlalleri için loglama özelliği kapatılabilmelidir.
d- Log bilgileri oturum ve oturum açmada kullanılan bilgileri (login identifiers) içermelidir.
e- Hassas bilgilerin loglanması maskelenebilmeli/örtülebilmelidir (suppress).

3.3. Teklif edilecek WAF çözümü, mevcut güvenlik politikası tarafından başlangıçta saldırı olarak kabul edilen meşru talepleri izinli olarak tanıtmanın kolay bir yolunu sağlamalıdır (false positive).

3.4. Teklif edilecek WAF çözümü, güvenliğin içerik yönlendirme kuralları için yapılandırılmasında granüler yapılandırmalara izin vermelidir. Örn. Içerik yönlendirme için oluşturulan özel güvenlik kuralları.

3.5. Teklif edilecek WAF çözümü, SharePoint, Outlook Web erişimi, WordPress, Joomla, Drupal, Oracle uygulamaları gibi belirli uygulama platformları için hazır güvenlik politikaları sağlamalıdır.

3.6. Teklif edilecek WAF çözümü, özellikle atak logları olmak üzere tüm loglar için benzersiz bir kimlik numarası (log ID) sağlamalıdır.

3.7. Teklif edilecek WAF çözümü, istek veya yanıt trafiğinden false positive olanları ayıklamak ve öğrenmek için otomatik olarak akıllı buluşsal yöntemler (intelligent heuristics) kullanmalı ve güvenlik politikalarını değiştirerek false positivelerin azaltılmasını tavsiye edebilmeli ve gerçekleştirebilmelidir.

3.8. Teklif edilecek WAF çözümü, farklı uygulamalar için farklı ilkeler tanımlama yeteneği sağlamalı ve Outlook Web Access, SharePoint ve Oracle gibi yaygın uygulamalar için hazır ilkeler sağlamalıdır.

3.9. Teklif edilecek WAF çözümü yönetim modülü, tercihen bir regex aracı yardımıyla, korunan uygulamalar ile ilişkili benzersiz özel imzalar geliştirilebilmeisni sağlayabilmelidir.

3.10. Teklif edilecek WAF çözümü, yüksek düzeyde granüler yönetim sunmalıdır. Algılama (Monitor) modu ve önleme (prevention) modunda geçiş yapmak tüm uygulama ile ilişkilendirilmek zorunda olmamalı, uygulamanın her bir bileşeni ya da herhangi bir saldırı ile ayrıntılı olarak ilişkilendiriliebilmelidir.

3.11. Teklif edilecek WAF çözümü, kapsamlı bir profil öğrenme süreci sağlamalıdır.

3.12. Ayrılmış sorumlulukları desteklemek için birden fazla profil bulunmalıdır. Cihaz operatörleri (box yapılandırması için), uygulama sahipleri (ilke yapılandırması için), denetçiler (günlük incelemesi için), sertifika yöneticileri, ağ yöneticileri vb. Özel roller oluşturmak da mümkün olmalıdır. Bu tür RBA kullanıcılarının kimliklerini LDAP veya RADIUS gibi harici bir hizmetten doğrulamak mümkün olmalıdır.

3.13. Teklif edilecek WAF çözümü, IP veya IP adres aralığı olarak güvenilen kaynaklar (trusted host) belirtebilmelidir. Böylece belirtilen güvenilir kaynaklara politikaların engellediği aksiyonları alabilmeleri için izin verilebilmelidir.

3.14. Yönetim uygulaması tercihen özel yönetim arayüzlerinden hem HTTP hem de HTTPS erişimi olan Web Tabanlı bir arayüz içermelidir.

3.15. Teklif edilecek WAF çözümü, Chef, Puppet ve Ansible gibi popüler yapılandırma yönetimi araçlarını desteklemek için genişletilebilen JSON tabanlı bir REST API kullanılarak uçtan uca yapılandırılabilir olmalıdır.

3.16. Teklif edilecek WAF çözümü, yönetim erişimi için yerleşik Rol Tabanlı Erişim Kontrolünü desteklemelidir.

3.17. Teklif edilecek WAF çözümü, Rol Tabanlı Erişim Kontrolü için LDAP ve Radius desteklemelidir.

3.18. Teklif edilecek WAF çözümü, yönetim erişimi için Çoklu Kimlik Doğrulama (MFA) özelliğini desteklemelidir.

3.19. Teklif edilecek WAF çözümü, yönetici hesaplarına hak atanırken bu hakları okuma/yazma gibi granüler seviyede atamayı desteklemelidir.

3.20. Teklif edilecek WAF çözümü, aynı ya da farklı cihazda kullanılmak üzere güvenlik politikaları ve alt politikalar için şablon tabanlı bir yapılandırma yeteneğine sahip olmalıdır.

3.21. Teklif edilecek WAF çözümü, tüm cihazları merkezi olarak yönetebilmelidir.

3.22. Teklif edilecek WAF çözümü, SIEM çözümleri ile kolayca entegre olabilmek için özelleştirilebilen log formatlarını desteklemelidir.

3.23. Teklif edilecek WAF çözümü, Vulnerability Scan (zafiyet tarama) araçları ile uyumlu çalışmalıdır.

3.24. Teklif edilecek WAF çözümü, kendi Vulnerability Scan aracı ile zamanlamış ya da manuel şekilde, dışarıdan tarama yaparak açıkları raporlayacak ve WAF üzerinde bu açıklar için tavsiye edilen

aksiyonlar görüntülenecektir. Istenen aksiyonların otomatik şekilde WAF üzerinde alınması desteklenmelidir.

3.25. Teklif edilecek WAF çözümü, SNMP trap desteğine sahip olmalıdır.

3.26. Teklif edilecek WAF çözümü, atak ve trafik raporları sağlamalıdır.
- a- Raporlar loglarda bulunan bilgilere göre özelleştirilebilmelidir.
- b- Raporlar manuel olarak oluşturulabilecekleri gibi zamanlanmış raporlar olarak FTP sunucuya çıkartılabilir ya da e-posta ile gönderilebilmelidir.

3.27. Teklif edilecek WAF çözümü, PCI atakları ve PCI uyumluluk raporları sağlayabilmelidir.

3.28. Teklif edilecek WAF çözümü, Splunk, HP Arcsight, Symantec Envision vb. gibi popüler SIEM çözümleriyle Syslog Entegrasyonunu kullanarak log analizini desteklemelidir.

3.29. Teklif edilecek WAF çözümü, logları Azure Event Hub'a göndererek log analizi ve raporlamayı desteklemelidir.

3.30. Teklif edilecek WAF çözümü, logları bir ElastiSearch, Logstash and Kibana stack yapısına göndererek log analizi ve raporlamayı desteklemelidir.

3.31. Teklif edilecek WAF çözümü, yapılandırma için yedekleme alanı desteklemeli ve yedekleme işlemlerini otomatik olarak başlatabilmeli ve yapılandırma dosyalarını local olarak depolayabilmelidir.

3.32. Teklif edilecek WAF çözümü, zamanlanmış yedekleme işleri ile yapılandırmanın yedeğini alabilmelidir.

3.33. Teklif edilecek WAF çözümü, aktif/aktif ve aktif/pasif HA desteklemelidir.

3.34. Teklif edilecek WAF çözümü, ağ sanallaştırmayı desteklemelidir. Böylece karmaşık yönlendirme yeteneklerini destekleyebilmeli ve sanal servislerin mantıksal network ayrımını yapabilmelidir.

3.35. Teklif edilecek WAF çözümü, trafik aggregation için Link Bonding desteklemelidir.

3.36. Teklif edilecek WAF çözümü, Link Failover ve Redundancy desteklemelidir.

3.37. Teklif edilecek WAF çözümü, GDPR uyumlu olmalıdır.

3.38. Teklif edilecek WAF çözümü, yanıt sayfalarının değiştirilebilmesine/özelleştirilebilmesine izin vermelidir.

3.39. Teklif edilecek WAF çözümü, özel bir merkezi yönetim sunucusu veya bir bulut hizmeti kullanarak Merkezi Yönetimi desteklemelidir.

3.40. Teklif edilecek WAF çözümü, yapılandırma şablonlarının içer/dışa aktarılmasını desteklemelidir.

4. XLM Güvenlik Duvarı

4.1. Teklif edilecek WAF çözümü, XML Web Hizmetlerinin yaygın web uygulamalarını ve XML'e özgü saldırılarla korunmasını desteklemelidir.

4.2. Teklif edilecek WAF çözümü, WS-I Basic spesifikasyonlarina uyumlulugun zorlanmasını mümkün kılmalıdır.

4.3. Teklif edilecek WAF çözümü, XML dokümanlarının doğrulanmasını desteklemelidir. Böylece XML DDoS ve injection (SQL, OS, XSS Injectin vb...) ataklarina karsi koruma sağlayabilmelidir.

4.4. Teklif edilecek WAF çözümü, bir WSDL şemasına göre SOAP mesajlarının, başlıklarının ve gövdesinin doğrulanmasını sağlamalıdır.

5. API Koruma (JSON)

5.1. Teklif edilecek WAF çözümü, JSON temelli API framework ve Web Servislerinin yaygin uygulama duzeyindeki tehditlere ve JSON'a ozel ataklara karsi korunmasini saglamalidir.

5.2. JSON payload dogrulanmasini desteklemelidir. Bu dogrulama limit kontrolu, JSON anahtar uzunlugunu ve maksimum obje derinligini icermelidir.

5.3. Teklif edilecek WAF çözümü, APı sunucuları koruyabilmek için, Open API spesifikasyon dosyalarının içe aktarılmasına izin vermeli böylece güvenlik kuralları otomatik oalrak oluşturulabilmelidir.

5.4. Teklif edilecek WAF çözümü, API isteklerine hiz sinrilamasi uygulayabilmelidir.

5.5. Teklif edilecek WAF çözümü, API istek metodlarini filtreleme opsiyonlari saglayabilmelidir.

5.6. Teklif edilecek WAF çözümü, API koruma ozelligi bir pozitif guvenlik modeli olarak yapılandırılabilmelidir.

6. Uygulama Yayınlama Yetenekleri

6.1. Teklif edilecek çözüm WAF ve Load Balancer özelliklerini aynı cihaz üzerinde bulundurmalıdır.

a- Back-End sunucularında in-band ve out-of-band uç nokta denetimi gerçekleştirebilmeli ve sunucu hatası tespit edilirse trafiği akıllı bir şekilde yeniden yönlendirebilmelidir.

b- Teklif edilecek çözüm, Round Robin, Weighted Round Robin ve Least Request metodlarını desteklemelidir.

c- Source IP, Cookie insert, Cookie passive, Http header, URL parameter gibi persistence metodlarını desteklemelidir.

6.2. Teklif edilecek WAF çözümü, farkli uygulamalara sahip icerikleri farkli uygulama sunucularina yönlendirmeyi desteklemelidir. Örneğin tüm imaj isteklerini bir sunucuya tüm scripting isteklerini başka bir sunucuya yönlendirebilmelidir.

a- Teklif edilecek WAF çözümü, ana uygulama yük dengeleme politikasından bağımsız olarak, belirli bir içerik icin birden fazla sunucu atanmasini ve bu sunucular arasinda yuk dengelemeyi destekleyebilmelidir.

6.3. Teklif edilecek WAF çözümü, giden yanıtlardan secilenlerin önbellege alinmasini desteklemelidir. Boylece aynı içeriğe yönelik sonraki istekler, sunucuya iletilmek yerine doğrudan WAF' tan sunulabilmelidir.

6.4. Teklif edilecek WAF çözümü, ayrintılı icerikler icin giden yanıtların, veri yolu ihityacini azaltmak amaciyla sıkıştırılmasını desteklemelidir. Sıkıştırma içerik tipi temelli olarak belirtilebilmelidir, örn. Javascript, XML vb... olarak.

7. Kullanıcı Erişim Denetimi

7.1. Teklif edilecek WAF çözümü, uygulama sunucuları için (onların yerine) kullanıcı kimlik doğrulama işlemlerini yapabilecektir. Kullanıcı oturum açma ve oturum kapatma sayfaları değiştirilebilecek/özelleştirilebilecektir.

7.2. Kimlik doğrulama modülü LDAP, Radius vb. harici kimlik doğrulama dizinleri ile çalışabilmelidir.

7.3. Teklif edilecek WAF çözümü, istemci SSL sertifikası ve şifre ya da RSA Secure ID kullanarak 2 faktörlü kimlik doğrulama desteklemelidir.

7.4. Teklif edilecek WAF çözümü, kimlik doğrulama işleminden sonra istemcilerin yetkillerinin bulunduğu farklı sayfalara ulaşabilmeleri için yetkilendirme politikaları yapılandırabilmelidir. Örn. LDAP ile kimlik doğrulaması yapan Grup A kullanıcıları “/toplantinotları/* “ na erişirken grup B kullanıcıları “/partners/*”a erişebilmelidir.

7.5. Teklif edilecek WAF çözümü, korunan farklı web uygulamaları arasında Single Sign On desteklemelidir.

7.6. Teklif edilecek WAF çözümü, gerektiğinde denetim / sorun giderme amacıyla, kullanıcı kimliğini belirterek, kullanıcının tüm oturumlarını (eksiksiz istek ve yanıt gövdeleri) ve aksiyonlarını izlemek mümkün olmalıdır.

7.7. Teklif edilecek WAF çözümü, SAML' i destekleyen kimlik doğrulama mekanizmalarını kullanarak kullanıcı trafiğinin doğrulanmasını desteklemelidir

7.8. Teklif edilecek WAF çözümü, SAML kimlik doğrulaması için Single Sign On ve Single Logout işlevlerini desteklemelidir.

7.9. Teklif edilecek WAF çözümü, ADFS kimlik ve erişim denetimi kullanarak kullanıcı trafiğinin doğrulanmasını desteklemelidir.

7.10. Teklif edilecek WAF çözümü, OKTA kimlik denetimi kullanarak kullanıcı trafiğinin doğrulanmasını desteklemelidir.

7.11. Teklif edilecek WAF çözümü, OpenID Connect kullanan kimlik sağlayıcılarla entegrasyonu desteklemelidir.

7.12. Teklif edilecek WAF çözümü, kimlik doğrulama politikasının bir parçası olarak OpenID Connect ayarlarında özel talepleri desteklemelidir.