



**IZFAS**  
İZMİR FUARI • İZMİR FAIR

**İZMİR BÜYÜKŞEHİR BELEDİYESİ**  
**İZMİR FUARCILIK HİZMETLERİ KÜLTÜR VE SANAT İŞLERİ TİCARET A.Ş.**

**TEKLİF İSTEME MEKTUBU**

**Teklif İsteme Tarihi : 13/02/2020**

**Teklif No : 2020 / 95**

SIRA NO:	SATIN ALINACAK MAL ve/veya HİZMETİN CİNSİ	Miktar	Birim	Marka	B.Fiyat (K.D.V. Hariç)	Tutar (K.D.V. Hariç)
1	GÜVENLİK DUVARI ALIMI İŞİ. (3 YILLIK)	1	ADET			

**TESLİM SÜRESİ ..... TAKVİM GÜNÜ**

Yukarıda belirtilen mal ve/veya hizmet satın alınacaktır. Bu işe alaka gösterdiğiniz takdirde, aşağıdaki şartlar çerçevesinde tanzim edeceğiniz iş bu teklif isteme mektubunu, İdareмі Satınalma Müdürlüğü'ne imzalı ve kaşeli olarak; kapalı zarf içinde elden, faks (teyit alınız), e-posta olarak gönderilmesini rica ederiz.

**TEKLİF VERME VE SATINALMAYA İLİŞKİN HUSUSLAR:**

- Teklifinizi en geç **18/02/2020 saat 15:00**'a kadar İZFAŞ Satınalma Müdürlüğü'ne gönderiniz.
  - Adres : Zafer Mahallesi 840 Sokak Fuar Alanı Apt. No:2 Gazıemir / İZMİR
  - E-posta : [satinalma@izmirfair.com.tr](mailto:satinalma@izmirfair.com.tr)
  - Faks : 0.232.497 11 90-87
  - Tel : 0.232.497 11 85-86-88-89
- Teklifinizi, K.D.V. hariç birim fiyat ve toplam tutar olarak TL (Türk Lirası) bazında veriniz. Teklif mektubunun ve varsa teknik şartnamenin her sayfasını kaşelleyip imzalayınız. Teklif ettiğiniz mal/hizmet için orijinal veya dengi ürüne ait marka ve garanti süresini belirtiniz. Garanti süresi belirtilmeyen teklifler için mevzuattaki geçerli süreler kabul edilecektir.
- Teklif mektubunuzda teklif edilen mal ve/veya hizmetin toplam tutarı; 4734 sayılı Kamu İhale Kanunu Doğrudan Temin Usulü ile yapılan alımlarda, 3/g İstisna alımlarında, diğer alımlar veya diğer ihale usulleriyle ihale edilmesine karar verilmesi halinde yaklaşık maliyet tespitinde değerlendirileceğinden son fiyatınızı yazınız.
- Teklif süresi:** Teklif mektubundaki fiyatlar, son teklif verme tarihinden itibaren 30 (otuz) takvim günü süreyle geçerli olacaktır.
- Teslim adresi:** İdarenin Ambarına teslim edilecektir.
- Teslim süresi:** Taahhüt edilen mal ve/veya hizmet, ektteki şartnamede ve/veya sipariş formu ile belirtilen teslim süresinde teslim edilecektir. Teklif mektubunuzda belirteceğiniz teslim süreleri "takvim günü" olarak belirtilecektir. İş günü olarak belirtilen teslim süreleri "takvim günü" olarak değerlendirilecektir.
- İdare istediği takdirde, mal ve/veya hizmet alımları için sözleşme yapacak, teminat alacak ve oluşacak damga vergisi yüklenici tarafından ödenecektir.
- Kesin Teminat:** İdarece istenilmesi durumunda, sözleşme imzalanmadan önce yüklenici tarafından sözleşme bedelinin en az % 6 (yüzde altı)'sı oranında kesin teminat verilecektir. Teminat tutarının nakit olarak verilmesi durumunda, İdarenin belirteceği banka hesabına dekontunun üzerine sözleşme konusu alımın bilgileri yazdırılarak yatırılacaktır.
- Ödeme:** Mal ve/veya hizmetin teslimi ve kabulüne müteakip ekli şartnamelerde aksine bir süre yoksa en geç 30 (otuz) gün içinde ödeme yapılacaktır. Ödemelerde "borcu yoktur" belgesi yüklenici tarafından ibraz edilecektir.
- Diğer Hususlar:** Teklif veren istekli/istekliler, yukarıdaki şartlarla birlikte varsa teknik şartname ve/veya numunede istenen özellikler aynen kabul etmiş sayılır. İdare mal ve/veya hizmeti alıp almamakta veya bir kısmını almakta serbesttir.

**EK – Teknik Şartname**

**TEKLİF VEREN FİRMANIN/KİŞİNİN:**

Adı, Unvanı :  
Adres :  
Tel/Faks :  
Vergi/T.C. No :

## TEKNİK ŞARTNAME

### 1. İŞİN KONUSU VE KAPSAM

1.1. Bilgi İşlem Müdürlüğü'nün ihtiyacı doğrultusunda güvenlik duvarı teknik şartnamesidir.

### 2. SATIN ALINACAK MAL KALEMLERİN LİSTESİ

SIRA NO	CİNSİ	TOPLAM
1	GÜVENLİK DUVARI	1 ADET

### 3. GÜVENLİK DUVARI TEKNİK ŞARTNAMESİ

- 3.1. Teklif edilecek Cihaz, bu şartname de belirtilen ve ek lisanslama gerektiren özellikleri hariç tüm fonksiyonları ile 3 (üç) yıl lisanslı olarak teklif verilecektir.
- 3.2. Teklif edilecek cihaz, mevcutta kullanılmakta olan hotspot yazılımına uygun olacaktır, hotspot yazılımına uygunluk ile ilgili ek bir ücret talep edilmeyecektir
- 3.3. Teklif edilecek Cihaz 3 (üç) yıl süre ile donanım garantisine sahip olacaktır. 3 (üç) yılın sonunda lisans yenilemesi yapılması durumunda cihaz donanım garantisi de devam edecektir (5 yıla kadar).
- 3.4. Teklif edilecek Cihaz üzerindeki tüm servisler 3 (üç) yıl süre ile lisanslı olarak teklif edilecektir.
- 3.5. Talep edildiği takdirde, ürüne APT saldırılarını engelleme amaçlı lisans da sağlanabilmelidir
- 3.6. Teklif edilen ürün IPv6 desteklemeli ve IPv6 Ready Gold sertifikasına sahip olmalıdır.
- 3.7. Teklif edilen ürünün Stateful packet inspection, deep packet inspection, proxy firewall özelliği olmalıdır.
- 3.8. Teklif edilen Güvenlik Duvarı; web arayüzü, Windows yönetim yazılımı ve command line arayüzü üzerinden yönetilebilir olmalıdır. Tüm yönetim yazılımları firewall ile aynı marka olmalıdır.
- 3.9. Güvenlik duvarı çözümleri, raporlama yazılımı ve yönetim modülü aynı ve tek marka olmalıdır. İnternete çıkan trafiği kontrol altına alarak , antivirus , anti-spyware , IPS ve spam blocking ile içerdeki kullanıcıları korumalıdır.
- 3.10. UTM kullanılarak güvenlik servisleri , antivirüs koruması IPS , içerik filtreleme ,spam control ve VPN site-to-site ve uzak kullanıcılar bir cihazda toplanır.
- 3.11. Teklif edilecek güvenlik duvarı çözümleri, raporlama yazılımı ve yönetim modülü aynı ve tek marka olmalıdır.
- 3.12. Ürün ICSA Firewall, ICSA IPsec VPN ve Common Criteria EAL4+ sertifikalarına sahip olmalıdır.
- 3.13. Teklif edilen Ağ Güvenlik Duvarı Sistemi, güncel "Unified Threat Management" için "Gartner Magic Quadrant 2014" tablosunda liderler kategorisinde yer almalıdır ve bu yüklenici tarafından belgelendirilmelidir.
- 3.14. External, private and optional (DMZ) olmak üzere üç farklı zone u desteklemelidir.
- 3.15. 8.0 Gbps firewall throughput and 800 Mbps UTM throughputunu desteklemelidir.
- 3.16. 3,300,000 eş zamanlı oturumu, saniyede 48,000 yeni oturumu desteklemelidir.
- 3.17. UTM kapsamında , URL filtreleme, IPS, GAV ve sıfır gün tehditlerine karşı önlem alabilmelidir.
- 3.18. Uygulama katmanında (Layer 7), proxy kuralları ile uygulama katmanında kontrol sağlamalıdır.
- 3.19. Uygulama katmanı proxyleri en çok kullanılan protokolleri önceden configure edilmiş default ayarlar ile desteklemeli; HTTP, HTTPS, POP3, SMTP, FTP, DNS, SIP, H.323.
- 3.20. RADIUS sunucu , SecureID ,LDAP ve Active Directory ve kendi veri tabanı ile kimlik doğrulama yapabilmelidir.
- 3.21. Active Directory sunucusu ile Single-Sign-On desteklenmeli.

Uğur ÇÖZÜMLER  
Bilgi İşlem Sorumlusu

Gökhan ARIKAN  
Bilgi İşlem Müdürü



- 3.22. Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.
- 3.23. Dinamik DNS 'i desteklemelidir.
- 3.24. Cihaz, donanımsal arıza riskini en aza indirme amaçlı olarak Hard Disk bulundurmamalıdır.
- 3.25. Fragment ataklar için önlem alabilmeli, paketler iç networke geçmeden tekrar birleştirebilmelidir.
- 3.26. Yaygın kullanılan protokollerde içerik çeşidi kontrolü yapabilmeli, bunu MIME içerik çeşidi ile yapabilmelidir.
- 3.27. DoS ve DDOS ataklarına karşın önlem alabilmelidir.
- 3.28. Mobile VPN'i desteklemelidir
- 3.29. Mobile VPN IPSEC 100 kullanıcıyı desteklemelidir
- 3.30. Mobile VPN SSL /L2TP 100 kullanıcıyı desteklemelidir.
- 3.31. Sistem üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır.
- 3.32. SSL VPN istemcisi en az Windows, Mac OS cihazları desteklemelidir.
- 3.33. Ofisler arası VPN 'i desteklemelidir. (Branch - Branch)
- 3.34. Ofisler arası en az 100 IPSEC VPN tünel adedini desteklenmelidir.
- 3.35. IPSEC için diğer marka ürünler ile standart çalışmayı desteklemelidir
- 3.36. IPSEC için tanımlama mekanizması DES, 3DES, AES 128 -, 192 -, 256-bit 'i desteklemelidir.
- 3.37. IPSEC için SHA-1, MD5, IKE Pre-Shared Key, 3rd Party Cert. şifrelemeyi desteklemelidir.
- 3.38. VPN Failover desteklenmelidir.
- 3.39. VPN throughput değeri en az **4.6 Gbps** olmalıdır.
- 3.40. Önerilen sistem 802.1q tabanlı VLAN desteklemelidir.
- 3.41. Güvenlik Duvarı üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir.
- 3.42. Farklı kullanıcı, kullanıcı grupları, ip ve ip gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.
- 3.43. Proxy kurallarında (harici URL )exception girilebilmelidir.
- 3.44. URL filtreleme uyarı ekranları özelleştirilebilecektir.
- 3.45. Uygulama Kontrolü için önceden tanımlı 1800+ imzaya sahip olmalıdır.
- 3.46. Uygulama imzalarının otomatik ve düzenli güncellenmesi gerekmektedir.
- 3.47. Aynı kutuda anti-virus fonksiyonu desteklemelidir.
- 3.48. Antivirüs imzaları otomatik update edilmelidir.
- 3.49. Antivirus e-mail için karantinaya sahip olmalıdır
- 3.50. Antivirus belirli domainlerden gelebilecek güvenli mailler için whitelisi desteklemelidir.
- 3.51. Spyware bloklama yapabilmelidir.
- 3.52. Sıkıştırılmış dosyaları (. Zip,. Tar, .rar, gzip) tarayabilmelidir.
- 3.53. HTTP, FTP, SMTP, POP3 gibi tüm ana protokolleri desteklemelidir.
- 3.54. Bulut bazlı reputation servisi ile puanı 1-100 arası olanlar antivirus taramasına gerek duymamalı, böylece sistem performansı artırılmış olmalıdır.
- 3.55. Servis, kötü itibarlı siteleri (geçmiş viruslu, spam ya da zararlı yazılımlar) buluttan bilgi olarak engellemelidir.
- 3.56. Anti virüs kapasitesi en az 3 Gbps olmalıdır.
- 3.57. Aynı kutuda Anti-spam özelliği desteklenmelidir
- 3.58. Anti spam teknolojisi Recurrent Pattern Detection (RPD) içermelidir.
- 3.59. Antispam karantina opsiyonunu desteklemelidir.
- 3.60. Antispam ve antivirus birlikte çalışabilmelidir.
- 3.61. IPS Servisi, teklif edilen çözüme entegre olarak bulunmalıdır .

- 3.62. IPS imzaları için otomatik update yapılabilmelidir.
- 3.63. IPS ile uygulama katmanında analiz yapılabilirmeli ,atak seviyelerini değerdendirip , alarmları üretebilmelidir.
- 3.64. IPS servisi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir.
- 3.65. Tüm ana protokolleri desteklemelidir; HTTP, FTP, SMTP, POP3.
- 3.66. IPS kapasitesi en az 4.8 Gbps olmalıdır.
- 3.67. IPS Servisi Full Scan veya Fast Scan (hızlı tarama) yapacak şekilde konfigüre edilebilmelidir.
- 3.68. NAT ve PAT desteklenmelidir.
- 3.69. İçerdeki sunucular için yük dengeleme (load balancing) desteklenmelidir.
- 3.70. Static NAT (Port Forwarding) desteklenmelidir.
- 3.71. Dynamic NAT desteklenmelidir.
- 3.72. Bire bir NAT(One-to-One) desteklenmelidir.
- 3.73. Kural Bazlı NAT desteklenmelidir.
- 3.74. Interface sayısı **8 adet 10/100/1000** olmalıdır.
- 3.75. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli olarak kullanabilmelidir.
- 3.76. Birden fazla WAN bağlantısı RoundRobin, Failover, Interface Overflow olarak konfigüre edilebilmelidir.
- 3.77. En az 200 adet VLAN oluşturulabilmelidir.
- 3.78. Kullanıcı, kural, protokol , arayüz ve grup bazlı bant genişliği kontrolü sağlamalıdır.
- 3.79. Cihaz; router mode i drop-in mod ve ve transparnt bridge moda'a alınabilir olmalıdır.
- 3.80. Statik, Dinamik NAT 'ı ve 1-1 NAT 'ı desteklemelidir.
- 3.81. Ürün High-Availability özelliğinde çalışabilmelidir. High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir.
- 3.82. Admin tarafından belirlenecek parametrelere bağlı olarak hangi dış arayüzden internete çıkılacağına karar verebilmelidir.
- 3.83. Sistemin SPI(Stateful Packet Inspection) ve DPI ( Deep Packet Inspection ) Firewall özelliği olmalıdır.
- 3.84. Teklif edilen Güvenlik Duvarı; web arayüzü, windows yönetim yazılımı ve command line arayüzü üzerinden yönetilebilir olmalıdır.
- 3.85. Teklif edilen ürün IPv6 desteklemeli ve IPv6 Ready Gold sertifikasına sahip olmalıdır.Gerçek zamanlı trafik log takibi yapabilmelidir.
- 3.86. Ürünün SSH ve SNMP v2/v3 desteği olmalıdır.
- 3.87. Donanım platformu 64 bit olmalıdır.
- 3.88. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.
- 3.89. Önerilecek sistem kendi üzerinde veya raporlama yazılımı aracılığı ile raporlama yapabilmelidir.
- 3.90. Loglama ve Raporlama yazılımı güvenlik duvarı ile aynı marka olmalıdır.
- 3.91. Raporlama yazılımı pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine gönderebilmelidir.
- 3.92. Güvenlik duvarı farklı sistem ve uygulamalara syslog gönderebilmelidir.
- 3.93. Teklif edilecek çözüm, CryptoLocker benzeri yeni nesil saldırıları engelleme amaçlı olarak, mevcut cihaza ek lisanslama yapılarak koruma altına alınabilmelidir.
- 3.94. Teklif edilecek çözüm, istek halinde ek bir lisanslama ile Gateway DLP çözümü işlevini de üstlenebilmelidir.

Uğur ÇÖMÜKLER  
Bilgi İşlem Sorumlusu

Gürkan ARKAN  
Bilgi İşlem Müdürü



#### 4. ALIMIN GERÇEKLEŞMESİ SÜRECİ, ŞARTLARI VE GECİKME CEZASI

- 4.1. Yüklenici, İZFAŞ tarafından onaylanmış işbu teknik şartnameye aynen uymakla yükümlüdür.
- 4.2. Yüklenici, teknik şartnameye konu olan malzemelerin tamamını tam ve eksiksiz biçimde teslim etmekle yükümlüdür.
- 4.3. Mal zamanında teslim edilmediği takdirde, İZFAŞ tarafından Yükleniciye 1(bir) iş günü süreli yazılı ihtar gönderilecektir. İhtar süresi içerisinde teslim edilecek işbu teknik şartname konusu mal ile ilgili, gecikilen 1 (bir) iş günü bakımından Yükleniciye yapılacak ödemelerden, toplam teklif bedeli üzerinden %5 (Yüzde Beş) Oranında para cezası kesilecektir. İZFAŞ tarafından belirlenen ihtar süresi içinde teslimin hiç gerçekleştirilmemesi durumunda işbu teknik şartnameye konu mal alımı İZFAŞ tarafından iptal edilecektir.
- 4.4. Yukarıda anılan gecikme cezaları, Yükleniciye ayrıca protesto çekmeye gerek kalmaksızın ödemelerden kesilecektir.
- 4.5. Mezkûr cezanın ödemelerden karşılanmaması halinde Yüklenicinin varsa, mevcut tüm alacakları veya teminatlarından (cari alacak- mevcut ise teminat mektubu) tahsil edilecektir.
- 4.6. Yüklenici, işbu teknik şartnameye konu mal alımının iptali sebebiyle, İZFAŞ'tan hiçbir nam altında herhangi bir hak talebinde bulunamaz.

#### 5. DENETİM MUAYENE VE KABUL İŞLEMLERİ

- 5.1. Muayene ve kabul işlemleri daha önce kurulmuş olan muayene ve kabul komisyonu tarafından yapılır.
- 5.2. Aksi belirtilmedikçe satın alınan mal/ hizmet Yüklenici tarafından sözleşmede ve/ veya teknik şartnamede belirtilen teslim yerine teslim edilmedikçe muayene ve kabul yapılamaz.
- 5.3. Yüklenici sözleşmenin ayrılmaz parçası olan teknik şartnamede de belirtildiği üzere tüm işler bittikten sonra İZFAŞ'a teslimine müteakip, İZFAŞ tarafından görevlendirilen 3 personel ile oluşacak kabul komisyonunca kabulüne dair tutanak düzenlenecek ve kabul işlemi gerçekleştirilecektir. Komisyon tarafından görülen eksiklikler, yüklenici tarafından komisyonun öngördüğü süre içerisinde giderilecek ve komisyon tarafından incelendikten sonra kabul yapılacaktır.

Uğur ÇUBUKLER  
Bilgi İşlem Sorumlusu

Gürkan ARIKAN  
Bilgi İşlem Müdürü