

**ÜSKÜDAR ÜNİVERSİTESİ**

**BİLGİSAYAR VE GÜVENLİK DUVARI ALIMLARI**

**TEKNİK ŞARTNAMESİ**

#

# **Giriş ve Amaç**

Üsküdar Üniversitesi, Türkiye’nin yeniliğe açık, eğitim sektöründe markalaşmayı önem veren bir “Kurum” dur. Bu kurum, verdiği eğitimin kalitesi ile diğer tüm kurumlardan ayrışmakta ve yetiştirdiği insanlar ile ülkemizin iyi bir yere gelmesinde önemli bir rol oynamaktadır.

Bu önemli misyonu gereği kurumun verdiği eğitim, eğitimin ve bilginin sunumu, bilgiye erişim ve bilginin korunması gibi normal kurumlardan farklı davranması gereken bazı konular bulunmaktadır.

Üsküdar Üniversitesi bilgiyi hem öğrencilerine sunmakta hem de kurum içinde hizmet kalitesi ve iç işleyişinin devamlılığı için kurum bünyesinde kullanmaktadır.

Üsküdar Üniversitesi bilgiyi sakladığı sunduğu sistemleri yenileme, iyileştirme ve bu altyapı ile ilgili ek ve bütünleyici hizmet ve ürün satın almaya dönük olarak bu şartnameyi oluşturmuştur.

# **Projenin Açıklaması ve Ön Kabuller**

Proje; kurumun altyapısındaki yazılım, sistem, sunucu, ağ yapısı gibi birçok noktaya hizmet veren servislerde yenileme, iyileştirme, kurulum, göç (migration) çalışmalarını içermektedir. Bu projede aşağıda teknik detayları verilen hizmetin alınması planlanmaktadır. Bununla birlikte şartnamenin genelinde belirtilen teknik detaylardan bağımsız olarak aşağıdaki şartların sağlanması olmazsa olmazdır.

* + Kurum, istediği şartlarda ve teknik özelliklerde değişiklik yapma hakkına veya bu projeyi komple iptal etme hakkına sahiptir. Bu değişikliği İstekli’lere bildirmek Kurum’un kendi insiyatifindedir.
	+ Kurum, gelen tekliflerdeki tüm kalemlerde hizmet almak yerine parçalı satın almayı da tercih edebilir. İstekli bunu peşinen kabul etmiş sayılır.
	+ Çözüm için önerilecek hizmet detayları, uluslararası ve yerel tüm standartlara üretici en iyi pratiklerine, sektör en iyi pratiklerine, gerek güvenlik, gerek performans tüm açılardan uyumlu olmalıdır. Standart dışı hiç bir yaklaşım, çözümlerde kullanılmamalıdır.
	+ İstekli, teklif vermeden önce çalışma yapılacak yeri ve sistemleri görebilir. Görmeden vereceği tekliflerin tamamında doğacak herhangi bir zarar ve ortaya çıkan bir eksikten İstekli ve eğer teklifi kabul olmuş ise “Yüklenici” sorumlu olacaktır.
	+ Çözümlerin bileşenlerinde hiçbir tek-hata-noktası (single-point-of-failure) olmamalıdır. Yani sistemdeki herhangi bir bileşende yaşanacak herhangi bir sorun, mutlak suretle sistemin kendi içindeki bileşenler ile telafi edilmeli ve sistem çalışır halde olabilmelidir. Aksi mümkün değilse İstekli, sunacağı teklif içeriğinde bunu net olarak belirtmelidir.
	+ Sistemin çalışabilmesi için gerekli olan tüm lisanslar, çözüm ile birlikte verilmelidir.
	+ Sistemin çalışabilmesi için gerekli olan tüm bağlantı kabloları, kartlar, ek modüller vb. çözüm ile birlikte eksiksiz bir şekilde verilmelidir.
	+ Aşağıda teknik detayları verilmiş bileşenlerin, birbirlerinden fiziksel olarak ayrı veya tek bir bütünsel yapıda olması, hedeflenen performans ve kapasite değerleri yakalandığı sürece Kurum tarafından aynı değerlendirilecektir. Hem geleneksel hem de bütünleşik çözümleri içerecek şekilde üretilmiştir.
	+ Üsküdar Üniversitesinin belirttiği şekilde ürünlerin kurulum ve montajları eksiksiz olarak Yüklenici tarafından yapılacaktır.

# **Genel Koşullar**

Bu ihale kapsamındaki işlerde Yüklenici ile Kurum arasında “GİZLİLİK” anlaşması yapılacaktır. Kapsam Kurum tarafından belirlenecektir.

**Ürünler stoklu ve hemen teslim olacaktır.**

Yüklenici, proje kapsamında Kurum tarafından belirlenen standart prosedürlere ve yönergelere uyumlu olacak şekilde hizmet verecek ve kayıtları Kurum’un göstereceği elektronik ortamda saklayacak, istendiğinde Kurum’a sunacaktır.

Yüklenici, kurumun talep ettiği ISO27001, ISO9001:2015 ve ISO20000-1:2011 sertifikasyonlara sahip olan firmalar tercih sebebidir.

Yüklenici, bu “Şartname” ve eklerinde belirtilsin veya belirtilmesin alacağı ve uygulayacağı kararlarda Kurum’un onayını alacaktır. Kurum, yazılı olmak kaydı ile yapılacak işlemler için süreçleri Yüklenici’ye devredebilir.

Yüklenici, çalışmalar sırasında sistemin kesintiye uğramaması için gerekli önlemleri alacak ve müdahaleye başlamadan önce Kurum’u bilgilendirecektir.

İstekli, teklif edeceği ürünlerle ilgili (Donanım, yazılım, lisans, Microsoft, Vmware, Veeam) üreticisinden veya yetkili distribütöründen bu ihale için alınmış şartname kapsamında teklif edilen ürünleri satmaya, kurmaya ve teknik desteğini vermeye yetkili olduklarını gösterir İstekli adına düzenlenmiş yetki belgelerini teklif ile birlikte Kurum’a sunacaktır.

Belirtilen ürün ve hizmetlerin bir bütün olarak çalışması için gerekli her türlü ek/yardımcı donanım ve hizmet Yüklenici tarafından sağlanacaktır. Sadece geçiş ve kurulum için gerekli olan ve geçiş sonrasında Kurum’un ihtiyacı olmayacak bir bileşen var ise onu da Yüklenici karşılayacaktır.

Tüm ürünler (donanım, yazılım, lisans vb.) yeni, kullanılmamış, hasarsız ve eksiksiz olarak, orijinal paketinde işin yapılacağı yere getirilecektir.

Projede kullanılacak olan tüm ürünlerin birbirleriyle uyumluluğu gözetilecektir. Projede öngörülen uygulamalarda ürünlerin herhangi bir nedenle (sürüm, standart uyuşmazlığı vb.) ortaya çıkan uyum sorunlarının giderilmesi yükümlülüğü Yüklenici’ye aittir.

Her türlü malzeme temini, işçilik ve uyumu Yüklenici sağlayacaktır. Bu şartnamede tarif edilmeyen ama sistemin çalışması için zorunlu olan tüm tamamlayıcı parçalar Yüklenici tarafından ücretsiz bir şekilde temin edilecek ve monte edilip çalışır hale getirilecektir.

Temin ve teslim edilecek her türlü malzemenin nakliye, taşıma, sigorta, geçici depolama sorumluluğu ve bunlara bağlı her türlü masraf, Yüklenici tarafından karşılanacaktır. Teslim ve kurulum yeri Kurum lokasyonudur.

Kurum, gerekli görmesi durumunda, kullanılacak ürünlerden numune isteyebilir veya Yüklenici’nin benzer ürünleri sattığı, hizmetleri sunduğu bir veya birkaç yerde yerinde inceleme yapmak isteyebilir. Yüklenici, talep edilmesi halinde bu istekleri yerine getirecektir.

İstekli teklifinde kullanacağı tüm cihazlar, malzemeler ve donanımlara ait marka ve modellerini liste halinde ve yoruma mahal bırakmayacak detayda (isim, ürün kodu, marka, model, alt model, bileşen detayı vb.) sunacağı teklif dökümanında yer verecektir.

Belirtilen tüm ürünler, kurulumu yapıldıktan sonra anahtar teslimi çalışır vaziyette teslim edilecektir.

İstekli, “Şartname”deki tüm maddeleri ayrı ayrı cevaplayacaktır. Hiçbir madde boş bırakılmayacak, cevaplar açık, anlaşılır, yeterli teknik düzeyde olacaktır. Sadece “**okunmuş, anlaşılmış ve kabul edilmiştir**” şeklinde verilen cevaplar kabul edilmeyecektir. Cevapların olması gereken yerde olmayışının ve/veya bulunamayışının ve bu nedenle değerlendirme yapılamamasının sorumluluğu teklif verene aittir.

Yüklenici, projelerde risk yönetimi uygulayacaktır. Proje boyunca yaşatacağı ve güncelleyeceği risk dokümanı ile olası risk, kesinti ve aksaklıklar için proaktif tedbir alınmasını sağlayacaktır. Risk yönetimi yaklaşımını Kurum, Yüklenici’ye iletecek ve gerekli doküman/şablon vb. Yüklenici ile paylaşacaktır.

Yüklenici, bu ihale kapsamındaki tüm çalışmalarında gerekiyor ise mesai saatleri dışında da (akşam, hafta sonu gibi) çalışacaktır.

Yüklenici, projenin her aşamasından sorumlu, bir proje yöneticisi belirleyecektir. Bu kişiye tatil günleri dâhil 7/24 ulaşılabilecektir.

Tüm çalışmalar için taslak proje planı ve süre, teklif ile birlikte kuruma sunulmalıdır.

Tüm çalışmalar aşağıdaki fazlardan geçerek uygulanacaktır. Aşağıdaki maddeler, bütünsel projenin her bir alt projesi için ayrı ayrı uygulanacaktır.

* + Kapsam ve Vizyon
	+ Planlama
	+ Geliştirme
	+ Kararlı Hale Getirme
	+ Yaygınlaştırma
	+ On-the-job training

Tüm çalışmalarda (her bir proje/danışmanlık için ayrı ayrı olacak şekilde) aşağıdaki dokümanlar üretilmeli ve teslim edilmelidir.

* + Kapsam ve Vizyon dokümanı
	+ Proje planı (Sürekli güncellenecek – mpp ve xlsx formatlarında)
	+ Risk dokümanı (Sürekli güncellenecek)
	+ Analiz dokümanı
	+ Planlama ve tasarım dokümanı
	+ Geçiş esnasında gerekecek prosedürler ve kontrol listeleri
	+ Haftalık ilerleme durum raporu

Tüm çalışmalarda aşağıdaki durumlarda toplantı yapılması gerekecektir.

* + Alt proje başlangıçlarında
	+ Kriz anında
	+ Tasarım ve geçişlerde gerektiği zaman
	+ Kurum talep ettiği zaman

# **İhtiyaç**

Yüklenici, Kurum’a aşağıdaki ihtiyaçlar doğrultusunda çözüm önerecek ve kabulü ardından bunun uygulamasını yapacaktır.

1. **AIO PC TEKNİK ŞARTNAME**
	1. **TÜMLEŞİK BİLGASAYAR MODEL 1 ( 16 adet)**
		1. Ürün markanın kurumsal ürün serisinde bir ürün olacak ve bu talep halinde marka tarafından onaylanabilecektir.
		2. Teklif edilecek tümleşik bilgisayarın ekranı parlama yapmayan 23.8” Full HD 250 NITS IPS panel olacaktır.
		3. Teklif edilecek bilgisayar üzerinde en az 11. Nesil i7-1165G7 işlemci bulunacaktır.
		4. Ürün üzerinde 16GB tek slotta ram ile gelecek
		5. Ürünün üzerindeki depolama alanı en az 256GB PCIE G3 SSD ve 1TB SATA disk olmalıdır.
		6. Teklif edilecek bilgisayar, içindeki anakart ile aynı marka olacak ve BIOS’u bilgisayar üretici firmaya ait olacaktır.
		7. Teklif edilecek bilgisayar üzerinde MX330 2GB ekran kartı olacaktır.
		8. Bilgisayarın dahili web kamerası ve mikrofonu olacaktır, sonradan eklenen kameralar kabul edilmeyecektir.
		9. Ürün üzerinden 1 adet USB 2.0 Tip-A, 4 adet USB 3.2 Gen 1 Tip A port bulunacaktır. Ayrıca 1 adet RJ45 ve 1’er adet adet HDMI-in ve HDMI-out port bulunmalıdır. Dönüştürücüler kabul edilmeyecektir.
		10. Ürünün 802.11ac destekleyen Wifi5 kartı olacak ve çift bant Bluetooth bağlantısına olanak tanıyacaktır. Ürün gigabit bağlantı desteklemelidir.
		11. Ürün ile birlikte aynı marka kablosuz klavye ve mouse verilecek, sonradan yapıştırma marka ve serigrafi yapılmış ürünler kabul edilmeyecektir.
		12. Ürün ve beraberinde verilecek olan aksesuarlar siyah ve tonlarında olmalıdır.
		13. Ürünün güç ünitesi en az 90W olacaktır.
		14. Kutusuz ağırlığı 5.5kg’dan fazla olan ürünler kabul edilmeyecektir.
		15. Ürün boyutları en fazla 54 x 40.9 x 4.8 cm olmalıdır.
		16. Ürünlerde Winpro İşletim sistemi olacaktır.
	2. **TÜMLEŞİK BİLGASAYAR MODEL 2 ( 112 adet)**
		1. Teklif edilecek ürün markanın kurumsal ürünleri arasında olacaktır ve üzerinde herhangi bir işletim sistemi kurulu olmayacaktır.
		2. Ürün markanın kurumsal ürün serisinde bir ürün olacak ve bu talep halinde marka tarafından onaylanabilecektir.
		3. Teklif edilecek tümleşik bilgisayarın ekranı parlama yapmayan 23.8” Full HD 250 NITS LCD panel olacaktır.
		4. Teklif edilecek bilgisayar üzerinde en az 11. Nesil i7-1165G7 işlemci bulunacaktır.
		5. Ürün üzerinde 16GB tek slotta ram ile gelecek,
		6. Ürünün üzerindeki depolama alanı en az 512GB PCIE G3 SSD olmalıdır.
		7. Teklif edilecek bilgisayar, içindeki anakart ile aynı marka olacak ve BIOS’u bilgisayar üretici firmaya ait olacaktır.
		8. Teklif edilecek bilgisayar üzerinde Intel dahili ekran kartı bulunacaktır.
		9. Bilgisayarın dahili web kamerası ve mikrofonu olacaktır, sonradan eklenen kameralar kabul edilmeyecektir.
		10. Ürün üzerinden 1 adet USB 2.0 Tip-A, 4 adet USB 3.2 Gen 1 Tip A port bulunacaktır. Ayrıca 1 adet RJ45 ve 1’er adet adet HDMI-in ve HDMI-out port bulunmalıdır. Dönüştürücüler kabul edilmeyecektir.
		11. Ürünün 802.11ac destekleyen Wifi5 kartı olacak ve çift bant Bluetooth bağlantısına olanak tanıyacaktır. Ürün gigabit bağlantı desteklemelidir.
		12. Ürün ile birlikte aynı marka kablolu klavye ve mouse verilecek, sonradan yapıştırma marka ve serigrafi yapılmış ürünler kabul edilmeyecektir.
		13. Ürün ve beraberinde verilecek olan aksesuarlar siyah ve tonlarında olmalıdır.
		14. Ürünün güç ünitesi en az 90W olacaktır.
		15. Kutusuz ağırlığı 5.4kg’dan fazla olan ürünler kabul edilmeyecektir.
		16. Ürün boyutları en fazla 54 x 40.9 x 16.5 cm olmalıdır.
		17. Ürünlerde Winpro İşletim sistemi olacaktır.
	3. **TÜMLEŞİK BİLGASAYAR MODEL 3 ( 22 adet)**
		1. Ürün markanın kurumsal ürün serisinde bir ürün olacak ve bu talep halinde marka tarafından onaylanabilecektir.
		2. Ürün üzerinde donanımsal TPM chipseti bulunmalıdır.
		3. Teklif edilecek tümleşik bilgisayarın ekranı parlama yapmayan 21.5” Full HD 250 NITS IPS parlama yapmayan 16:9 panel olacaktır.
		4. Teklif edilecek bilgisayar üzerinde en az 10. Nesil i7-10510U işlemci bulunacaktır.
		5. Ürün üzerinde 8GB tek slotta RAM ile gelecek, ürün üzerinde boşta bir ram slotu daha bulunacaktır.
		6. Ürünün üzerindeki depolama alanı en az 256GB PCIE G3 SSD olmalıdır. Sata SSD diskler kabul edilmeyecektir.
		7. Teklif edilecek bilgisayar, içindeki anakart ile aynı marka olacak ve BIOS’u bilgisayar üretici firmaya ait olacaktır.
		8. Teklif edilecek bilgisayar üzerinde Intel tümleşik ekran kartı bulunacaktır.
		9. Bilgisayarın dahili web kamerası ve mikrofonu olacaktır, sonradan eklenen kameralar kabul edilmeyecektir.
		10. Ürün üzerinden 2 adet USB 3.2 Tip-A, 2 adet USB 2.0 Gen 1 Tip A port bulunacaktır. Bunlara ek olarak 1 adet USB 3.2 Tip-C port istenmektedir. Dönüştürücüler ve USB çoklayıcılar kabul edilmeyecektir. Ayrıca 1 adet RJ45 ve en az 1 adet HDMI-out port bulunmalıdır. Dönüştürücüler kabul edilmeyecektir.
		11. Ürünün 802.11aC destekleyen Wifi5 kartı olacak ve çift bant Bluetooth bağlantısına olanak tanıyacaktır. Ürün gigabit bağlantı desteklemelidir.
		12. Ürün ile birlikte aynı marka kablolu klavye ve mouse verilecek, sonradan yapıştırma marka ve serigrafi yapılmış ürünler kabul edilmeyecektir.
		13. Ürün ve beraberinde verilecek olan aksesuarlar beyaz/gümüş ve tonlarında olmalıdır.
		14. Ürünün güç ünitesi en az 90W olacaktır.
		15. Kutusuz ağırlığı 6.4kg’dan fazla olan ürünler kabul edilmeyecektir.
		16. Ürün boyutları en fazla 48.9 x 42.5 x 0.7 cm olmalıdır.
		17. Ürünlerde Winpro İşletim sistemi olacaktır.
	4. **WORKSTATION BİLGİSAYAR & MONİTÖR ( 31 adet )**
		1. Teklif edilen kişisel bilgisayar üreticinin iş istasyonu ürün ailesine ait olmalıdır.
		2. Teklif edilen kişisel bilgisayarın tüm bileşenleri (kasa, anakart, monitör, klavye, mouse) üreticiye ait olacaktır.
		3. Teklif edilen kişisel bilgisayarın; güvenlik (safety) için UL, CSA veya EN sertifikalarından en az birisine, ergonomi için TUV veya GS sertifikalarının en az birine ve CE belgesine sahip olacaktır. Bu sertifikalar belgelendirilecektir.
		4. Teklif edilen kişisel bilgisayarı oluşturan parçalar bilgisayar üreticisi tarafından üretilmiş olmalıdır ya da üreticisi firmanın ürün koduna sahip olmalıdır.
		5. Teklif edilen kişisel bilgisayarın anakartı bilgisayarla aynı marka olacaktır ve anakart üzerinde üretici firmanın orjinal logosu bulunacaktır. Kazınmış, silinmiş ya da çıkartmalı logoya sahip anakartlar kesinlikle kabul edilmeyecektir. Anakart üzerinde bulunan BIOS üreticiye ait olacaktır. Sistem açıldığında BIOS üreticisi ile sistem üreticisinin aynı olduğu BIOS ayarlarından gösterilecektir.
		6. Teklif edilen kişisel bilgisayarın chipseti Intel W580 chipset veya üst modeli olacaktır.
		7. Teklif edilen kişisel bilgisayarın işlemcisi 11. nesil Intel i9 serisi en az 8 çekirdek, baz / temel frekansı en az 2.5 Ghz, turbo frekansı en az 5.2 Ghz ve ön belleği en az 16 MB olmalıdır.
		8. Teklif edilen kişisel bilgisayarın sistem belleği en az 32 GB 3200 MHz DDR4 olacaktır ve 4 adet DIMM bellek yuvası bulunacaktır. Bellek miktarı en az 128 GB’a kadar yükseltilebilmelidir. 16GB ‘lık kitlerle de teklif edilebilir.
		9. Teklif edilen kişisel bilgisayarın üzerinde en az 512 GB PCIe NVMe SSD disk bulunacaktır. Bu diskin sıralı okuma hızı minimum 3335 MB/s, yazma hızı ise minimum 2360 MB/s olmalıdır.
		10. Teklif edilen sistem 3 adet 3.5” ya da 4 adet 2.5” disk destekleyen yuvaya sahip olmalıdır.
		11. Teklif edilen sisteme aynı anda 3 adet 2280 M.2 PCI NVMe SSD takılabilmelidir.
		12. Sistem standart olarak 4 adet SATA 3.0 bağlantı noktasına sahip olmalıdır.
		13. Teklif edilen kişisel bilgisayarın üzerinde min. Nvidia RTX A4000, 16GB, 4DP

ekran kartı bulunacaktır.

* + 1. Teklif edilen kişisel bilgisayarın BIOS ayarlamaları yetkisiz kullanıcıların sistemi açmalarını engellemek amacıyla, parola (power on password) imkânına elverişli olacaktır.
		2. Teklif edilen kişisel bilgisayar üzerinde anakarta entegre WOL ve PXE destekli 10/100/1000 Mbps ethernet kartı bulunmalıdır.
		3. Teklif edilen kişisel bilgisayar üzerinde 8x DVD+/-R/W yazıcı bulunacaktır.
		4. Teklif edilen kişisel bilgisayar üzerinde entegre TPM 2.0 yonga seti bulunmalıdır.
		5. Teklif edilen kişisel bilgisayar üzerinde entegre ses kartı olacaktır.
		6. Teklif edilen kişisel bilgisayar üzerinde en az 1 adet tam boy ve 300W ekran kartlarını destekleyen PCIe x16 Gen4, en az 1 adet tam boy PCIe x4 Gen3 ve 1 adet tam boy PCI-32 genişleme yuvası olacaktır.
		7. Teklif edilen bilgisayar kasası minitower veya tower yapıda olmalıdır. Ön tarafta SD kart okuyucu bulunmalıdır.
		8. Teklif edilecek masaüstü bilgisayarın en az 1 (Bir) adet PS/2 mouse portu, en az 1 (Bir) adet PS/2 klavye portu ve anakart üzerinde en az 2 adet DisplayPort 1.4 ve 1 adet HDMI 2.0 görüntü çıkışı bulunacaktır.
		9. Teklif edilen kişisel bilgisayarda en az 4 adedi ön tarafta, en az 5 adedi arka tarafta olmak üzere en az 9 adet USB girişi olmalıdır. USB portlardan en az 3 adedi USB 3.2 Gen2 ve en az 1 adedi USB 3.2 Gen 2x2 (20Gbps)Type-C olmalıdır. USB portları sağlamak için herhangi çoğaltıcı ya da dönüştürücü kullanılmayacaktır.
		10. Teklif edilen kişisel bilgisayar entegre ses kartına sahip olacak kasasının ön tarafında bütünleşik mikrofon ve kulaklık girişi, arkasında da ses çıkışı olacaktır.
		11. Teklif edilecek masaüstü bilgisayarın kasasına kullanılan güç ünitesi kasa içinde kullanılan tüm üniteleri sorunsuz destekleyecek ve ilave bir güç ünitesi gerektirmeyecektir.
		12. Teklif edilen kişisel bilgisayarın kasası, kasa içerisine dışarıdan müdahaleye engel olacak şekilde anahtarlı kilit mekanizmasını destekleyecek yapıya sahip olacaktır.
		13. Teklif edilen kişisel bilgisayarla birlikte 1 adet USB bağlantılı Türkçe Q standart klavye ve 1 adet USB optik mouse verilecektir.
		14. Teklif edilen kişisel bilgisayarın güç kaynağı en az 460W güçte ve en az %90 verimli çalışma özelliğinde olacak ve en az 80PLUS Gold sertifikasına sahip olmalıdır.
		15. Teklif edilen kişisel bilgisayarda Windows 10 Pro for Workstations 64bit (6 Cores plus) işletim sistemi yüklü olmalıdır.
		16. Teklif edilen kişisel bilgisayarlar en az 3 yıl yerinde üretici garantili olacaktır. Bu üreticinin destek web sitesinden görüntülenebilmelidir.
		17. Teklif edilen taşınabilir bilgisayarlar, “Energy Star” ve “EPEAT Gold” sertifikasına sahip olmalıdır. “EPEAT Silver” uyumluluğu http://www.epeat.net sitesinden alınacak çıktı ile belgelendirilmelidir.
		18. Teklif edilen markanın sunulan modeli UL, GS (TUV), FCC, CB ve CE sertifikalarından en az ikisine sahip olacaktır.
		19. Sistem çalışırken normal halde operatöre gelen en yüksek ses seviyesi 29.7 dB olmalıdır. Bu değer işlemci yüükü ağır olduğunda en yüksek 35.7 dB olmalıdır.
		20. Sistem performansını kullanılan uygulamaya göre otomatik olarak en iyi hale ayarlayan yapay zeka destekli yazılıma sahip olmalıdır.
		21. Depolama kullanımını kullanılan uygulamaya göre otomatik olarak en iyi hale ayarlayan yapay zeka destekli yazılıma sahip olmalıdır.
		22. Teklif edilen bilgisayar için 31 adet 31.5’’ monitör de teklife dahil edilmelidir.
		23. Teklif edilen monitorün max. çözünürlüğü 2560 x 1440 at 60Hz olmalıdır
		24. Teklif edilen monitorun konektörleri 1 x DP port 1 x HDMI port 1 x USB Type-C upstream port, 2 x USB 2.0 downstream port - Back 2 x SuperSpeed USB 5Gbps (USB 3.2 Gen1) şeklinde olmalıdır.
		25. Teklif edilen monitorun ayarlanabilir standı olmalıdır.
		26. Teklif edilen monitorun ENERGY STAR®, EPEAT® sertifikaları olmalıdır
1. **AĞ GÜVENLİK DUVARI SİSTEMİ VE MERKEZİ YÖNETİM SİSTEMİ**
	1. **AĞ GÜVENLİK DUVARI SİSTEMİ**
		1. Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.
		2. Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;
		3. Güvenlik Duvarı (Firewall)
		4. IPSec VPN Sonlandırma Sistemi
		5. SSL VPN Sonlandırma Sistemi
		6. Saldırı Tespit ve Engelleme Sistemi (IPS)
		7. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
		8. Virüs/Zararlı İçerik Kontrolü
		9. URL Kategori Filtreleme
		10. Bant genişliği yönetimi
		11. Özelliklerine sahip olmalıdır.
		12. Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlamalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.
		13. Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, her hâlükârda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.
		14. Teklif edilen Ağ Güvenlik Duvarı High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.
		15. Yedeklilik konfügrasyonunda her segment için güvenlik duvarı üzerinde set edilecek Ip sayısı 1 (bir) adet olmalıdır. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.
		16. Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.
		17. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır
		18. Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN’lar arayüz (interface) olarak kullanılabilmelidir.
		19. Sistem Sanal Güvenlik Duvarı özelliği ile kullanıldığı durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilmelidir.
		20. Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.
		21. Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
		22. SPI (stateful packet inspection),
		23. Saldırı Tespit ve Engelleme Sistemi (IPS)
		24. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
		25. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
		26. URL Kategori Filtreleme
		27. Routing modda aşağıdaki özellikleri sağlamalıdır;
		28. SPI (stateful packet inspection),
		29. IPSec VPN Sonlandırma,
		30. SSL VPN Sonlandırma,
		31. Saldırı Tespit ve Engelleme Sistemi (IPS)
		32. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
		33. Virüs/Zararlı İçerik Kontrolü
		34. URL Kategori Filtreleme
		35. Bant genişliği kontrolü
		36. Statik yönlendirme (static routing),
		37. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
		38. Sunucu yük dengeleme
		39. WIFI Access Point kontrolcüsü
		40. WAN optimizasyon
		41. Web Cache
		42. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.
		43. Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.
		44. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.
		45. Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü ve/veya zone bazlı yazılabilmelidir.
		46. Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.
		47. Kullanıcı bazında NAT kuralı yazılabilmelidir.
		48. Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.
		49. Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
		50. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
		51. İstenildiğinde tek IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural dahilinde izin verilmiş olan tüm kaynak IP lerin herbiri için, tanımlanan bant genişliğinin ve/veya max eşzamanlı oturum sayısının garanti edilmesi sağlanmalıdır.
		52. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
		53. Uygulama bazında bant genişliği kontrolü yapabilmelidir.
		54. Aynı trafik ile ilgili Inbound ve outbound doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.
		55. Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.
		56. Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları gibi tanımlı en az 3.000 (üçbin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.
		57. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.
		58. Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.
		59. IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilmelidir.
		60. Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapan IP adresinin olası diğer saldırıları başlamadan engellenmiş olmalıdır.
		61. Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkân sağlamalıdır.
		62. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.
		63. Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.
		64. Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.
		65. SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.
		66. SSL VPN özelliği en az 5.000 kullanıcı lisansı ile teklif edilecektir.
		67. SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.
		68. SSL VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, Bant Genişliği yönetimi (QoS) özellikleri uygulanabilir olmalıdır.
		69. Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3 trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment’leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir
		70. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.
		71. Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.
		72. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı URL filtreleme politikaları set edilebilmelidir.
		73. Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.
		74. Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.
		75. URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin \*.gov.tr\* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.
		76. İstenildiğinde categorilerden bağımsız olarak, sisteme eklenebilecek tam URL bilgisi (Örneğin: [www.abc.com/deneme/sayfa1.php](http://www.abc.com/deneme/sayfa1.php)) bazında engelleme yapabilmelidir
		77. Https üzerinden erişilmeye çalışılan domain adreslerinin (örneğin www.abc.com) engellemesi sertifika kullanımı olmadan gerçekleştirilebilmelidir.
		78. SSL trafiğini kendi üzerinde yaratılan bir sertifikayı yada farklı bir CA den alınmış yeterli özelliklere sahip bir sertifika ile inceleyebilmelidir. Bu sayede sadece domain bazında değil, URL bazında (Örneğin: [www.abc.com/deneme](http://www.abc.com/deneme)/test.php) engelleme yapabilmelidir. URL kategorileri bazında SSL incelemeye girmeyecek domainler belirlenebilmelidir.
		79. URL filtreleme uyarı ekranları özelleştirilebilecektir.
		80. Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir.
		81. Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
		82. Seri bağlantı ile konsol port üzerinden,
		83. Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
		84. SSH bağlantı ile komut satırı (commandline) üzerinden
		85. Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir.
		86. Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.
		87. Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.
		88. Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, “NSS Labs Network IPS” ve “NSS Labs Next Generation Firewall” testlerine girmiş olması gereklidir.
		89. Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel “Enterprise Firewall” için “Gartner Magic Quadrant” tablosunda yer almalıdır.
		90. Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.
		91. Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.
		92. Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP, Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.
		93. Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.
		94. HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.
		95. SSL bağlantıları için SSL Offloading özelliği olmalıdır.
		96. Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:
		97. Kaynak Ip hash bilgisi
		98. Round robin
		99. Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak
		100. Aktif durumda olan gerçek sunuculardan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi
		101. Ping paketlerine verilen cevaplar esas alınması
		102. Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin <http://10.31.101.30/test_page.htm> adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.
		103. Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.
		104. Teklif edilen sistem wifi controller olarak çalışabilecek, bu sayede kullanılabilecek kablosuz erişim cihazlarının yönetimi için kullanılabilecektir.
		105. Wan optimizasyon özelliklerine sahip olacaktır.
		106. Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.
		107. Web cache özelliği olmalıdır.

# **Güvenlik Duvarı Performans Değerleri**

* + 1. Teklif edilen Ağ Güvenlik Duvarı 2 adet yedekli olarak teklif edilecektir.
		2. Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda en az 80 Gbps (512 byte UDP) Firewall performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
		3. Her bir Ağ Güvenlik Duvarı ünitesi Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az 7.1 Gbps kapasiteye sahip olmalıdır. Bu kapasite kullanıcı/istemci arasındaki istek-cevap trafiğinin toplamına (çift yönlü analiz ile) bu güvenlik özelliklerinin uygulandığı konfigürasyonda belirlenmiş olmalıdır. Belirtilen bu değer ürün kataloglarında yer almalıdır. Ürün kataloglarında Tehdit Koruma için farklı terminoloji kullanılmış ise bu koşulda ürün kataloğunda NGFW (Firewall + IPS + Uygulama Denetimi) kapasitesi gerçek ortam değeri baz alınarak en az 9.8 Gbps olmalıdır.
		4. Sistem aynı anda en az 8 milyon oturumu desteklemeli ve saniyede en az 500.000 yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
		5. Güvenlik Duvarı Sistemi en az 48 Gbps IPSec VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
		6. Sistem Site-to-Site için en az 5.000 adet, Client to site için 10.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir.
		7. Sistem üzerinde;
		8. En az 2 adet 40GE QSFP+ ara yüz bulunmalıdır.
		9. En az 4 adet 25GE SFP28 ara yüz bulunmalıdır.
		10. En az 4 adet 10GE SFP+ ara yüz bulunmalıdır.
		11. En az 8 adet 1GE SFP ara yüz bulunmalıdır.
		12. En az 18 adet 1GE RJ45 ara yüz bulunmalıdır.
		13. Sistemin; Firewall ve IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.
	1. **Forti Manager - MERKEZİ YÖNETİM SİSTEMİ**
		1. Çözüm ile hem merkezdeki hemde şubelerdeki cihazları merkezi olarak yönetilebilecektir.
		2. Çözüm sanal veya fiziksel appliance olarak teklif edilebilir.
		3. Çözüm en az 10 adet cihazı yönetebilecek şekilde tekliflendirilecektir.
		4. Merkezi yönetim çözümü ile yönetilen cihazlardaki bütün konfigürasyon objeleri tanımlanabilecek ve ilgili politikalar merkezi olarak oluşturulup cihazlara uygulanabilecektir.
		5. Merkezi yönetim çözümü ile beraber, yerel veya uzakta bulunan firewall veya accespoint cihazların otomatik olarak devreye alınması için gerekli “Zero Touch Provisioning” lisansı verilmelidir.
		6. Merkezi yönetim çözümü cihazların üzerindeki konfigleri çekebilecektir.
		7. Merkezi yönetim çözümünün cihazlar arasındaki VPN bağlantılarının merkezi konfigürasyonunun yapılmasına ve monitor edilmesini yarayan bir modulu olmalıdır.
		8. Merkezi yönetim çözümü üzerinde hiçbir ayar olmayan cihazların kendisine ulaşamasına ve daha önceden belirlenmiş şablonlara göre konfigürasyon basılmasını (Zero Touch Provisioning) destekleyecektir.
		9. Merkezi Yönetim yazılımı çok sahiplilik desteği ile bir den çok gruba farklı yetkilerle hizmet edebilmelidir (Multi-Tenancy)
		10. Merkezi yönetim yazılımı yeni politikaların uygulanaması yada olan politikalarda değişiklik yapılması sürecinin gözden geçirilmesini, onaya tabi olmasını ve audit edilmesini destekleyecektir.
		11. Merkezi Yönetim yazılımı üzerinde merkezi imza veritabanı oluşturulabilir ve her bir cihazın internet üzerinden ayrı ayrı imza ve diğer güncel güvenlik verilerini çekmesi yerine merkezi olarak kendi üzerinden çekilmesini desteklemelidir.
		12. Merkezi yönetim yazılımı restful API ile harici uygulamalar ile entegre olabilecektir.Bu sayede harici sistemler merkezdeki ve şubelerdeki cihazlardan API aracılığı ile veri çekebilecekler ve konfigürasyon değişikliklerini gerçekleştirebileceklerdir.
		13. Yukarıda belirtilen seçeneklerden hangisi ile teklif edilirse edilsin, teklif edilen sistemlerin en az 3 yıl yazılım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

# **Kayıt ve Raporlama Sistemi**

* + 1. Önerilen güvenlik duvarı sisteminin kayıt depolama ve takibini, raporlama işlemlerini gerçekleştirmek için aşağıda belirtilen şartlara uyan kayıt takip ve raporlama ürün/ürünleri alınacaktır.
		2. Aşağıda belirtilen özellikler yönetim ve kayıt sistemlerinin ayrı veya tek bir sistem olarak önerilmesi durumunda da sağlanacaktır.
		3. Önerilen sistem, saniyede en az 5 GB/Gün log kayıt alabilmelidir.
		4. Log kayıt alanı olarak en az 3 TB depolama alanını desteklemelidir.
		5. Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.
		6. Cihaz üzerinden geçen tüm trafiğin günlüklerde tutulması, istenen kıstaslara göre (En az IP, IP aralığı, ağ, protokol, zaman) filtrelenebilmesi ve aktif bağlantıların gerçek zamanlı izlenebilmesi sağlanacaktır.
		7. Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.
		8. Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilmelidir.
		9. Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.
		10. Merkezi yönetim dâhilinde bulunan bileşenlere ait anlık ortalama CPU, boş disk alanı, firewall, firewall cluster üzerinden akan tüm uygulamalar, kullanıcı IP adresleri ve dâhili kullanıcı isimleri gibi değerler anlık ve sürekli olarak görüntülenebilecektir.
		11. Önerilen kayıt yönetim sistemi geçmişe yönelik olarak raporlama yapabilme özelliğine sahip olacaktır. Örneğin bant genişliği kullanımı, uygulama denetimi, URL filtreleme ile ilgili istenen tarih aralıklarında raporlar üretebilecektir
		12. Tutulan kayıt alanları baz alınarak özelleştirilmiş sorgular yazılabilmeli ve bu sorguların çıktıları, tablo, pie-chart şeklinde raporlar içerisine konulabilmelidir.
		13. pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.
		14. Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek kayıtların yedekliliği sağlayabilmelidir.
		15. Yukarıda belirtilen seçeneklerden hangisi ile teklif edilirse edilsin, teklif edilen sistemlerin en az 3 yıl yazılım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir
1. **FİNANSAL BİLGİLER**

* 1. **ZAMAN TABLOSU**

###

* + 1. Aşağıdaki tarih tablosuna uygun olarak teklifler değerlendirilecektir. Bu tarihler, Üsküdar Üniversitesi iş yoğunluğu, beklentileri doğrultusunda değiştirilebilir.
		2. Üsküdar Üniversitesi, ihtiyaçlar doğrultusunda gerek kapsamda gerekse hizmette ek revizeler isteyebilir ve tarih tablosunu buna göre düzenleyebilir.

|  |  |
| --- | --- |
| **Proje Adı** | IT Altyapısı Projesi |
| **Teklif İsteme Başlangıç Tarihi** |  |
| **Teklif Verme Son Tarih** |  |
| **Tekliflerin İlk Değerlendirmesinin Sonuçlanması ve Revize İstenmesi** |  |
| **Revize Tekliflerin Değerlendirilmesi Son Tarih** |  |
| **Projenin Sonlandırılması** |  |
| **Hizmet Başlangıç Hedefi** |  |

* 1. **FİRMA TARAFINDAN DOLDURULACAK TABLOLAR**
		1. Aşağıdaki tablolar, ayrı bir dokümanda doldurularak Üsküdar Üniversitesi ile paylaşılmalıdır. Teklif vermek isteyen firma, aşağıdaki tablodaki bilgilerin haricinde ek şartlarını ve koşullarını, aşağıdaki bilgileri içermesi kaydı ile ekler halinde belirtebilir.
		2. Üsküdar Üniversitesi, referans olarak gösterilen proje/firmaları ziyaret etmek isteyebilir. Teklif veren firma, Üsküdar Üniversitesinin istemesi durumunda bu firmalara ziyaret planlamakla yükümlüdür.
		3. Yüklenici, en az 3’er adet referans sağlamalıdır.

**TEKLİF PARA BİRİMİ**

* + 1. Hizmet için verilen teklifler USD cinsinden verilmelidir.

|  |  |
| --- | --- |
| **Teklif Veren Firma** |  |
| **Teklif Tarihi** |  |
| **Proje Adı** |  |

|  |  |  |
| --- | --- | --- |
| **Hizmet / Ürün** | **Birim Fiyat (TL/Ay)** | **Toplam Fiyat** |
|  |  |  |
| **TOPLAM** |  |

|  |  |
| --- | --- |
| **Benzer Referanslar ve Projeler** | **Detaylar (Sunucu ve cihaz adedi, proje özeti)** |
| **Referans Müşteri Adı 1 :****Referans Proje Adı :** |  |
| **Referans Müşteri Adı 2 :****Referans Proje Adı :** |  |
| **Referans Müşteri Adı 3 :****Referans Proje Adı :** |  |

* 1. **KABUL ŞARTLARI**
		1. Proje, tüm bileşenleri ile bitirildiği zaman Kurum tarafından kabul işlemi yapılacaktır. Projenin kabulü yapılmadan bitmiş sayılmayacaktır. Kabul şartları aşağıdaki gibidir.
		2. Teklifteki tüm cihazlar eksiksiz bir şekilde kurulmuş çalışıyor olmalı
		3. Tüm sanal makineler yeni yapıya taşınmış olmalı
		4. Tüm danışmanlıklar verilmiş olmalı
		5. Tüm yedekleme ve iş sürekliliği sistemlerinde tam fonksiyonel testler yapılmış olmalı
		6. Tüm sistemler, sorunsuz 30 gün boyunca çalışıyor olmalı
		7. Tüm eğitimler verilmiş olmalı
		8. Projeye ait tüm dokümanların Kurum’a teslim edilmiş olması