# Dijital İhracat Kalesi Projesi
# Teknik Şartnamesi

**İÇİNDEKİLER**

# 1 GENEL

## 1.1 AMAÇ

İşbu şartname, Türkiye İhracatçılar Meclisi (TİM) ve İhracatçı Birlikleri Genel Sekreterliklerinin bilgi teknolojileri altyapısını güçlendirme, veri güvenliğini en üst düzeye çıkarma ve operasyonel verimliliği artırma amacıyla ortak bir veri merkezi kurulumu ve yönetimini kapsamaktadır.

Amaç, sunucu, ağ ve güvenlik ekipmanlarının yanı sıra gerekli yazılım lisanslarının ortaklaştırılmasıyla maliyet etkinliğini sağlamak, siber güvenlik sistemleri ile veri merkezini uluslararası standartlara uygun hale getirmek ve ihracatçıların dijital dönüşüm süreçlerini desteklemek ve hızlandırmaktır.

Bu ortak veri merkezi, ihracatçıların dijital varlıklarını güvenli bir şekilde saklamalarını, işlemlerini hızlı ve etkin bir şekilde gerçekleştirmelerini ve küresel pazarda rekabet avantajı elde etmelerini sağlayacak bir 'Dijital İhracat Kalesi' olarak hizmet verecektir.

## 1.2 İHALE KISIMLARI

### **1.2.1** İHALE KISIMLARI

**KISIM I:** Kısaca TAM YATIRIM ya da CAPEX olarak adlandırılabilecek olan KISIM I, İhalenin ana amacını oluşturan tüm donanım, yazılım ve hizmetlerin satın-alımını kapsayan kısımdır.

**KISIM II:** Kısaca "BULUT BİLİŞİM ve BARINDIRMA" ya da "OPEX" olarak adlandırılabilecek olan KISIM II, KISIM I tamamlanana kadar yeni geliştirilen E-Birlik sisteminin üzerinde koşacağı sistem ve altyapı hizmetlerinin kiralanması olarak özetlenebilir. E-Birlik, İDARE'nin en önem verdiği TİM ve İhracatçı Birlikleri Genel Sekreterliklerince ihracatçıların temel üyelik ve gümrük beyanname işlemlerinin yürütüldüğü omurga yazılımıdır. Kısım II, İDARE'nin ihale sonlandıktan sonra tabi olduğu Satın-Alım usül ve esaslarına uygun şekilde I. Kısmın tamamlanması (ya da tamamlanamaması durumunda da geçerli olacak şekilde) ve kurulumların yapılıp teslimatların kabulüne kadar geçen süre boyunca İDARE'nin belirtilen sunucularını barındırma ve eksik tüm donanım parkının kiralanarak veri merkezi hizmeti verme işidir.

### **1.2.2** Kısım I ve Kısım II tekliflerinin ortak değerlendirilmesi

İstekliler tarafından ihale konusu işin tüm kısımları (KISIM I ve KISIM II) için ayrı ayrı teklif verilmesi gerekmektedir. İhalenin değerlendirmesinde İDARE, iki KISIM için de verilen teklifleri kullanacaktır. Dolayısı ile KISIM I'e en uygun teklifi veren istekli KISIM II için vereceği uygun olmayan bir teklif nedeni ile ihaleyi kaybedebilecektir.

### 1.2.3 Kısım II'nin bağımsız alınabilmesi

İDARE, satın-alma usül ve esaslarında yaşayabileceği herhangi bir sebepten dolayı ihaleyi kazanan istekli firmadan sadece KISIM II'yi alma hakkına sahiptir. İhale sonuçlandığında ilk etapta KISIM II için sözleşme imzalanacak olup YÜKLENİCİ bu kısmi alım kapsamındaki işleri, sözleşme ve ihale dokümanında belirtilen şartlar çerçevesinde yerine getirmeyi kabul ve taahhüt edecektir.

## 1.3 KISALTMA, TERİM VE TANIMLAR

| Kısaltma ve Tanım | | İlgi | Açıklama |
|---|---|---|---|
| TİM | : | Genel | Türkiye İhracatçılar Meclisi |
| Active Directory | : | Genel | Microsoft'un geliştirdiği ve Windows tabanlı işletim sistemlerinde kullanılan ağ üzerindeki kaynakları (kullanıcılar, bilgisayarlar, yazıcılar, sunucular, dosyalar, gruplar vb.) yönetmek ve bu kaynaklara erişimi denetlemek ve kullanıcı hesaplarını, parolaları ve diğer kimlik bilgilerini saklamak için kullanılan dizin hizmetidir. "Active Directory şifresi" bilgisayar açılışında girdiğiniz şifredir. |
| Bakanlık | : | Genel | T.C. Ticaret Bakanlığı |
| Birlik | : | Genel | 5910 numaralı kanun ile yetkilendirilmiş İhracatçı Birlik |
| İhracatçı Birlik | : | Genel | 5910 numaralı kanun ile yetkilendirilmiş İhracatçı Birlik |
| e-Birlik | : | Genel | TİM yönetiminde, İhracatçı Birlik tescili, üyelik gibi ana işlevleri olan omurga yazılım |
| Genel Sekreterlik | : | Genel | İhracatçı Birliklerin icrasını yöneten yapılar |
| İhracatçı Birlik | : | Genel | 5910 numaralı kanun ile yetkilendirilmiş İhracatçı Birlik |
| İstekli | : | Genel | İşbu şartnameye teklif veren tüzel kişi |
| Outlook | : | Genel | Genel olarak kullanılan e-posta uygulamasıdır. |
| Proje/Platform | : | Genel | E-Birlik Yazılımı |
| Şartname | : | Genel | İşbu Teknik Şartname |
| Taraflar | : | Genel | İdare ve Yüklenici birlikte “Taraflar” ve tek başına “Taraf” olarak anılacaktır. |
| Yüklenici | : | Genel | Şartnamede tanımlanan işi yapmak için sözleşme imzalayan istekli |
| EDR | : | Genel | Endpoint Detection and Response |
| SandBox | : | Genel | Sandbox, bir sunucu, ağ ve sistem ortamında potansiyel olarak güvenliği tehdit edebilecek uygulamaların veya kodların, ana sisteme zarar vermeden izole edilmiş ve kontrollü bir ortamda çalıştırılması ve test edilmesi anlamına gelir. Sandbox terimi, özellikle güvenlik amacıyla kullanılır ve uygulamaların, kodların veya dosyaların gerçek sistemde etkisini anlamadan önce izole bir alanda analiz edilmesini sağlar. |
| DLP | : | Genel | Data Loss Prevention |
| SSL | : | Genel | Secure Sockets Layer |
| SIEM | | Genel | Security Information and Event Management |
| Refurbished | : | Genel | Refurbished (Yenilenmiş) terimi, daha önce kullanılmış veya fabrika hatası gibi nedenlerle geri dönmüş ürünlerin, üretici veya yetkili bir servis tarafından detaylıca kontrol edilip, arızaları veya kusurları giderildikten sonra yeniden satışa sunulması anlamına gelir. Yenilenmiş ürünler, genellikle ilk el ürün kalitesine oldukça yakındır ve çoğu zaman garantili olarak satışa sunulur. Yenilenmiş ürünler, şu işlemlerden geçebilir:<br>**Onarım:** Arızalı parçaların değiştirilmesi veya düzeltilmesi.<br>**Temizleme ve Test:** Ürünlerin tüm fonksiyonlarının düzgün çalıştığından emin olmak için kapsamlı testlerden geçirilmesi.<br>**Ambalajlama:** Orijinal ambalajı yeniden hazırlanır ve aksesuarlar da eklenir.<br>Refurbished ürünler, sıfır ürünlerden daha uygun fiyatlıdır ve işlevsel olarak tamamen çalışır durumda olmaları sağlanmıştır. |
| Remarketed | : | Genel | Remarketed (Yeniden Pazarlanan) terimi, daha önce kullanılmış, kiralama süresi dolmuş veya iade edilmiş ürünlerin, herhangi bir onarım veya yenileme işlemine tabi tutulmadan, ya da sadece küçük iyileştirmeler yapılarak yeniden satışa sunulmasıdır. Bu ürünler genellikle:<br>• İkinci El veya az kullanılmış ürünlerdir.<br>• Daha düşük fiyat ile satılırlar, ancak garanti kapsamı yenilenmiş ürünlere göre daha az olabilir veya hiç olmayabilir.<br>• Remarketed ürünler, bazen birkaç küçük kozmetik çizik veya kullanım izleri taşıyabilir, ancak genellikle işlevsel açıdan sorunsuzdur. |
| Veri Depolama Sistemi FC, iSCSI ve SAS protokolleri | : | Veri Depolama Sistemi | Veri Depolama Sistemi başlığı altında geçen FC, iSCSI ve SAS protokolleri, veri depolama alanında kullanılan veri iletim protokolleridir. Her biri, veri depolama birimleri (örneğin, sunucular ve disk sürücüleri) arasında verilerin güvenli ve hızlı bir şekilde iletilmesini sağlar.<br>**FC (Fibre Channel):** Yüksek hızlı, optik veya bakır kablolar aracılığıyla veri merkezlerinde kullanılan bir SAN protokolü. Yüksek performans ve düşük gecikme sağlar.<br>**iSCSI:** IP tabanlı bir protokol olup, Ethernet ağı üzerinden veri depolama aygıtlarına erişim sağlar. Ekonomik ve kolay uygulanabilir.<br>**SAS (Serial Attached SCSI):** Seri bağlantı kullanarak yüksek hızlı veri aktarımı sağlar ve disk sürücüleri ile sunucular arasında güvenilir bir bağlantı sunar. |

| Kısaltma ve Tanım | | İlgi | Açıklama |
|---|---|---|---|
| RAID | : | Veri Depolama Sistemi | Redundant Array of Independent Disks, birden fazla sabit diski bir araya getirerek veri depolama kapasitesini artırmak, performansı iyileştirmek ve veri güvenliğini sağlamak için kullanılan bir teknoloji yöntemidir. RAID, verileri birden fazla diske dağıtarak veri kaybına karşı koruma sağlar ve veri okuma/yazma hızlarını artırabilir.<br>RAID'in temel amacı, birden fazla diskin birlikte çalışarak verilerin bir kısmını veya tamamını yedekli olarak saklaması ve bu sayede disklerden birinin arızalanması durumunda verilerin kaybolmasını önlemektir. Ayrıca RAID kullanımı, depolama sistemlerinde performansı artırır ve kapasitenin daha etkin kullanılmasına yardımcı olur.<br>**RAID Seviyeleri:**<br>**RAID 0:** Verileri birden fazla diske bölerek (striping) yazan bir RAID türüdür. Yüksek veri aktarım hızları sağlar ancak yedeklilik sağlamaz. Bir disk arızalanırsa tüm veriler kaybolur.<br>**RAID 1:** Verilerin her bir diske aynen kopyalanması (mirroring) esasına dayanır. Yüksek veri güvenliği sağlar, ancak disk kapasitesi yarıya düşer (her veri iki diskte saklanır).<br>**RAID 5:** Verileri ve hata kontrol bilgilerini birden fazla diske dağıtır. Yüksek okuma/yazma performansı ve yedeklilik sunar. En az üç disk gerektirir.<br>**RAID 6:** RAID 5'e benzer, ancak iki hata kontrol bloğu kullanarak daha fazla yedeklilik sağlar. Bu, aynı anda iki diskin arızalanmasına karşı koruma sağlar.<br>**RAID 10 (1+0):** RAID 1 ve RAID 0 kombinasyonudur. Verileri hem aynalar (mirroring) hem de bölerek (striping) saklar. Yüksek performans ve yedeklilik sağlar ancak daha fazla disk gerektirir. |
| SSD | : | Veri Depolama Sistemi | Solid-State Drive |
| SAS | : | Veri Depolama Sistemi | Serial-Attached SCSI |
| NL-SAS | : | Veri Depolama Sistemi | Near Line SAS |
| NVMe | : | Veri Depolama Sistemi | Non-Volatile Memory |
| SED seçenekleri | : | Veri Depolama Sistemi | Self-Encrypting Drive |
| LUN | : | Veri Depolama Sistemi | Mantıksal Alanlar (LUN)- Logical Unit Number |
| RIP, RIPng, BGP, OSPF ve IS-IS dinamik yönlendirme protokolleri | : | SAN Switch (Anahtar) | Genellikle IP tabanlı ağlarda kullanılan dinamik yönlendirme protokollerini ifade eden bu protokoller, yönlendiriciler arasında ağ yollarını belirlemek ve veri trafiğini optimize etmek için kullanılır. |
| QoS Queue | : | SAN Switch (Anahtar) | QoS (Quality of Service) Queue yani hizmet kalitesi kuyruğunu ifade eder. SAN switch'in donanım ve yazılım özelliklerine entegre edilmiş bir ek fonksiyon olan bu mekanizmalar SAN ortamlarında diğerlerinden daha ktirik ve önemli veri trafiklerinin (örnek: kritik veritabanı işlemleri) öncelik sırasına göre işlenmesi sağlayan yapılardır.<br>Daha yüksek önceliğe sahip veri paketlerinin ağ üzerinden daha hızlı geçişi ve gecikme veya veri kaybının azaltılması amaçlanır. SAN Switch üzerindeki QoS Kuyruğu, belirli türde trafiğe öncelik vererek ağ kaynaklarının daha verimli kullanılmasını ve kritik uygulamaların performansının garanti altına alınmasını sağlar. |
| ACL | : | SAN Switch (Anahtar) | Anahtar üzerinde, layer 2 seviyesinde MAC adresi, layer 3 seviyesinde IP protokol tipi ve layer 4 seviyesinde UDP/TCP port numarasına göre ACL oluşturulabilecektir. |
| QoS Queue | : | SAN Switch (Anahtar) | Anahtar, port başına en az 8 adet donanımsal bazlı QoS Queue'ya sahip olacaktır. |
| VLAN | : | SAN Switch (Anahtar) | VLAN (Virtual Local Area Network), fiziksel olarak aynı ağda bulunan cihazları, mantıksal olarak farklı ağlara ayırmak için kullanılan bir ağ teknolojisidir. VLAN, aynı ağ anahtarı (switch) üzerinde ya da birden fazla anahtara bağlı cihazları, sanki farklı fiziksel ağlarda çalışıyormuş gibi birden fazla sanal ağ segmentine ayırarak ağ trafiğini düzenlemeyi ve güvenliği artırmayı sağlar. |
| LAG | : | SAN Switch (Anahtar) | Anahtar üzerinde en az 100 adet Link Aggregation Group (LAG) oluşturulabilecek ve her bir grupta en az 32 adet port bulunabilecektir. |
| PIM-SM | : | SAN Switch (Anahtar) | Anahtar, PIM-SM protokollünü destekleyecektir. |
| DHCP Relay, DHCP snooping, DAI özellikleri | : | SAN Switch (Anahtar) | Anahtar, DHCP Relay, DHCP snooping, DAI özelliklerini destekleyecektir. |
| SNMP v2c / v3 ve SSH v2 | : | SAN Switch (Anahtar) | Anahtar, konsol portu, SNMP v2c / v3 ve SSH v2 üzerinden yönetilebilecektir. |
| sFlow | : | SAN Switch (Anahtar) | Anahtarın sFlow ya da benzer desteği bulunacaktır. |
| FTP | : | SAN Switch (Anahtar) | Anahtar, FTP, FTP veya TFTP aracılığı ile firmware güncellemesi ve konfigürasyon yedeklemesi yapılabilecektir. |
| FTP | : | SAN Switch (Anahtar) | Anahtar, FTP, FTP veya TFTP aracılığı ile firmware güncellemesi ve konfigürasyon yedeklemesi yapılabilecektir. |
| TFTP | : | SAN Switch (Anahtar) | Anahtar, FTP, FTP veya TFTP aracılığı ile firmware güncellemesi ve konfigürasyon yedeklemesi yapılabilecektir. |

| Kısaltma ve Tanım | | İlgi | Açıklama |
|---|---|---|---|
| Auto MDI/MDI-X | : | SAN Switch (Anahtar) | Anahtar Auto MDI/MDI-X özelliklerine sahip olmalıdır. |
| IGMPv1/v2/v3 Snooping | : | SAN Switch (Anahtar) | Anahtar IGMPv1/v2/v3 Snooping desteğine sahip olmalıdır. IGMP snooping tablosunda en az 1000 adet satır (entry) bulanabilmelidir. |
| IEEE 802.1X Port Güvenlik standardı | : | SAN Switch (Anahtar) | Anahtarlar ağ güvenliğini sağlamak amacıyla, ağa bağlanan kullanıcıların yetkilendirilmesi için IEEE 802.1X Port Güvenlik standardını desteklemeli ve RADIUS desteğine sahip olmalıdır. |
| RADIUS | : | SAN Switch (Anahtar) | Anahtarlar ağ güvenliğini sağlamak amacıyla, ağa bağlanan kullanıcıların yetkilendirilmesi için IEEE 802.1X Port Güvenlik standardını desteklemeli ve RADIUS desteğine sahip olmalıdır. |
| DHCP Snooping | : | SAN Switch (Anahtar) | Anahtarlar DHCP Snooping, DAI (Dynamic ARP Inspection) ve IP Source Guard desteklemelidir. |
| DAI (Dynamic ARP Inspection) | : | SAN Switch (Anahtar) | Anahtarlar DHCP Snooping, DAI (Dynamic ARP Inspection) ve IP Source Guard desteklemelidir. |
| IP Source Guard | : | SAN Switch (Anahtar) | Anahtarlar DHCP Snooping, DAI (Dynamic ARP Inspection) ve IP Source Guard desteklemelidir. |
| LLDP | : | SAN Switch (Anahtar) | Anahtar LLDP ve LLDP-MED destekleyecek, LLDP-MED – VoIP entegrasyonu yapılabilecektir. |
| LLDP-MED | : | SAN Switch (Anahtar) | Anahtar LLDP ve LLDP-MED destekleyecek, LLDP-MED – VoIP entegrasyonu yapılabilecektir. |
| LLDP-MED – VoIP entegrasyonu | : | SAN Switch (Anahtar) | Anahtar LLDP ve LLDP-MED destekleyecek, LLDP-MED – VoIP entegrasyonu yapılabilecektir. |
| Quality of Service (Auto-QoS) | : | SAN Switch (Anahtar) | Anahtar VoIP için otomatik Quality of Service (Auto-QoS) özelliğini desteklemelidir. |
| TACACS+ | : | SAN Switch (Anahtar) | Anahtara yönetim erişimi için Radius ve TACACS+ protokolleri desteklenecektir. AAA (Authentication, Authorization ve Accounting) yapısı içinde anahtar yöneticilerinin erişimi kontrol edilebilecek, girebilecekleri komutlar sınırlandırılabilecek ve yaptıkları işlemler kayıt altında tutulabilecektir. |
| Time Domain Reflectometry (TDR) | : | SAN Switch (Anahtar) | Anahtar Time Domain Reflectometry (TDR) destekleyecektir. |
| DDR4 ECC UDIMM | : | NAS DEPOLAMA ÜNİTESİ | Teklif edilen cihaz; en az 8 GB DDR4 ECC UDIMM belleğe sahip olacak. |
| SFP+ Ethernet kartı | : | NAS DEPOLAMA ÜNİTESİ | Teklif edilen cihaz üzerinde 2 portlu 10G SFP+ Ethernet kartı olacaktır. |
| FW, APP CONTROL, IPS, AV, ANTI-SPYWARE, ANTI-BOT, ZERO-DAY MALWARE | : | GÜVENLİK DUVARI | Sistem en az 6 Gbit/s Thread Prevention (FW, APP CONTROL, IPS, AV, ANTI-SPYWARE, ANTI-BOT, ZERO-DAY MALWARE) throughput performans değerine Enterprise trafic MIX veya gerçek trafik değeri olarak sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır. |
| Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları | : | GÜVENLİK DUVARI | 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. |
| SPI (Stateful Packet Inspection) | : | GÜVENLİK DUVARI | Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır. |
| CIFS | : | GÜVENLİK DUVARI | Common Internet File System: CIFS, Microsoft tarafından geliştirilen bir dosya paylaşım protokolüdür ve ağdaki cihazlar arasında dosya, yazıcı ve diğer kaynakların paylaşılmasını sağlar. Windows işletim sistemlerinde yaygın olarak kullanılır ve bir tür SMB (Server Message Block) protokolüdür. |
| FTP | : | GÜVENLİK DUVARI | File Transfer Protocol: FTP, ağ üzerinden dosya transferi için kullanılan bir protokoldür. Sunucu ve istemci arasında dosya göndermeyi veya almayı sağlar. Genellikle web geliştirme ve veri aktarımı süreçlerinde kullanılır. |
| HTTP | : | GÜVENLİK DUVARI | HyperText Transfer Protocol: HTTP, web tarayıcıları ve web sunucuları arasında veri iletişimi için kullanılan temel bir protokoldür. Web sayfalarının ve diğer kaynakların internet üzerinden erişilmesini sağlar. Dünya çapında web (World Wide Web) üzerinde temel veri iletim protokolüdür. |
| MAPI | : | GÜVENLİK DUVARI | Messaging Application Programming Interface: MAPI, Microsoft Exchange sunucuları ve e-posta istemcileri (örneğin Microsoft Outlook) arasında e-posta iletişimi sağlamak için kullanılan bir protokoldür. E-posta, takvim ve diğer iletişim bilgilerinin yönetilmesine imkan tanır. |
| TCP | : | GÜVENLİK DUVARI | Transmission Control Protocol: TCP, verilerin güvenli ve sıralı bir şekilde iletilmesini sağlayan, internetin temel iletişim protokollerinden biridir. Bağlantı odaklı bir protokoldür ve iki uç arasındaki veri akışının düzgün bir şekilde gerçekleşmesi için paketlerin kayıpsız ve doğru sıralamayla iletilmesini garanti eder. |
| ping/traceroute, TCP/UDP, HTTP/HTTPS, SMTP, POP3, IMAP, DNS, SSH, LDAP, JDBC, FTP | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | SIEM sistemi ping/traceroute, TCP/UDP, HTTP/HTTPS, SMTP, POP3, IMAP, DNS, SSH, LDAP, JDBC, FTP vb. gibi uygulama seviyesini de içeren servis kontrolü yapabilmelidir. Synthetic Transaction Monitoring (STM) |

| Kısaltma ve Tanım | | İlgi | Açıklama |
|---|---|---|---|
| Synthetic Transaction Monitoring (STM) | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | SIEM sistemi ping/traceroute, TCP/UDP, HTTP/HTTPS, SMTP, POP3, IMAP, DNS, SSH, LDAP, JDBC, FTP vb. gibi uygulama seviyesini de içeren servis kontrolü yapabilmelidir. Synthetic Transaction Monitoring (STM) |
| SNMP, WMI, VM SDK, OPSEC JDBC, Telnet, SSH, JMX | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Veri toplamak veya cihazlarla haberleşebilmek amacıyla aşağıdaki protokolleri desteklemelidir: |
| PCI-DSS | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Payment Card Industry Data Security Standard, kredi kartı bilgilerini işleyen, saklayan veya ileten kuruluşlar için geliştirilmiş bir veri güvenliği standardıdır. Kredi kartı bilgilerinin güvenliğini sağlamak ve bu bilgileri siber tehditlerden korumak amacıyla ödeme sistemlerinde güvenlik standartlarını belirler.<br>PCI-DSS standardı, kredi kartı bilgilerine yetkisiz erişimi önlemek, ödeme süreçlerinde güvenliği sağlamak ve dolandırıcılığı önlemek için belirli gereklilikler sunar. SIEM ürünleri, PCI-DSS uyumluluğunu sağlamak amacıyla ödeme işlemleri sırasında veri güvenliğini izler, şüpheli etkinlikleri tespit eder ve raporlar, böylece hassas müşteri verilerinin korunmasına katkıda bulunur. |
| HIPAA | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Health Insurance Portability and Accountability Act: Sağlık sektöründe kişisel sağlık bilgilerinin korunması ve gizliliğinin sağlanmasını düzenleyen ABD yasasıdır. SIEM ürünleri, HIPAA gerekliliklerine uygunluk sağlamak için sağlık verilerini izler ve raporlar. |
| SOX | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Sarbanes-Oxley Act: Finansal raporlama ve kurumsal şeffaflık sağlamak amacıyla çıkarılan ABD yasasıdır. SIEM, SOX uyumluluğu için finansal verilere erişimi izler ve uygunsuz etkinlikleri raporlar. |
| NERC | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | North American Electric Reliability Corporation: Kuzey Amerika'da elektrik üretimi ve dağıtımı yapan kuruluşların güvenlik ve uyumluluk standartlarını belirler. SIEM, bu standartlara uygunluk sağlamak için elektrik altyapısında güvenlik izleme sağlar. |
| FISMA | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Federal Information Security Management Act: ABD federal kurumlarının bilgi sistemlerini korumak amacıyla belirlenmiş bir bilgi güvenliği yasasıdır. SIEM, FISMA uyumluluğunu sağlamak için güvenlik kontrollerini ve olayları izler. |
| ISO | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | International Organization for Standardization: ISO 27001 gibi standartlar, bilgi güvenliği yönetim sistemleri için küresel standartları belirler. SIEM, ISO standartlarına uyum sağlamak için bilgi güvenliği olaylarını ve riskleri yönetir. |
| GLBA | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Gramm-Leach-Bliley Act: Finansal kuruluşların müşteri bilgilerini korumasını zorunlu kılan ABD yasasıdır. SIEM, müşteri verilerinin izlenmesi ve güvenlik açıklarının tespiti ile GLBA uyumluluğunu sağlar. |
| GPG13 | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Good Practice Guide 13: İngiltere hükümeti tarafından kamu sektöründe bilgi güvenliği sağlamak için yayımlanan rehberdir. SIEM, bu rehbere uygun olarak güvenlik olaylarının izlenmesini ve raporlanmasını sağlar. |
| SANS Critical Controls | : | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Siber saldırılara karşı en etkili güvenlik uygulamalarını belirleyen bir kontrol listesi olarak SANS Enstitüsü tarafından yayımlanmıştır. SIEM, bu kritik kontrolleri izleyerek güvenlik açıklarını önlemeye yardımcı olur. |

# 2 KISIM I – ORTAK VERİ MERKEZİ

## 2.1 İŞİN KAPSAMI

İşbu şartname Ana Veri Merkezi ve Felaket Kurtarma Merkezine geçiş için altyapıda kullanılacak donanım, yazılım, bilişim güvenliği ürünleri ve Veri Merkezi bulundurma hizmetlerinin alınması işidir. Temel olarak 5 ana mal ve hizmet kalemini içermektedir;

**I.** Donanım Tedariği
**II.** Veri Merkezi Barındırma Hizmeti
**III.** İnternet Hizmeti
**IV.** Yazılım Ürünleri ve Lisanslama Hizmeti
**V.** Yönetilen Hizmetler (Bakım, Destek, Kurulum ve Eğitim)

## 2.2 İŞİN SÜRESİ

İşbu şartnamenin Kısım I'ine dahil kapsam tedarik edilecek ve barındırılacak ürünlerin kurulumu ve ayağa kalkmış şekilde teslimi sözleşmenin imzalanmasını müteakip 120 takvim günü içinde anahtar teslim olarak tamamlanacaktır.

Operatör hizmetleri ile bakım-destek ve garanti süreçleri (ve bu hizmet ve süreçlere dair ödemeler) ürün teslim ve kurulumundan sonra İDARE'nin yapacağı kabul ile başlayacaktır.

## 2.3 FİYATLANDIRMA

Kısım I'e ait Operatör hizmetleri ve bakım bedelleri aylık olarak Türk Lirası bazında fiyatlandırılacak olup yılda bir kere azami TÜİK'in açıklamış olduğu 1 yıllık (TEFE+YÜFE) /2 oranında fiyat arttırılacaktır.

## 2.4 GENEL

### 2.4.1 Genel Hükümler ve Detaylar

**2.4.1.1** Bu şartnamede belirtilen işlerin, tarif edildiği şekilde ve anahtar teslimi olarak tamamlanması esastır.

**2.4.1.2** İDARE'den kaynaklanacak gecikmeler yukarıdaki sürelere eklenecektir.

**2.4.1.3** YÜKLENİCİ, teklif edilen ihale bedelleri dışında fiyat farkı talep etmeyecektir. İşin kapsamının değişmesi durumunda idari şartnamenin ilgili koşulları uygulanacaktır.

**2.4.1.4** YÜKLENİCİ, proje aşamalarını, tüm mimariyi ve ürünleri teklifinde detaylandıracaktır.

**2.4.1.5** Ana Veri Merkezi Ağ altyapısı mimarisi, Bilişim Güvenliği altyapısı mimarisi, sunucu altyapısı mimarisi ve yedeklilik yapısı bu şartname başlıklarına uygun bir şekilde YÜKLENİCİ tarafından hazırlanıp teklifle birlikte sunulacaktır.

**2.4.1.6** FKM Veri Merkezi Ağ altyapısı mimarisi, Bilişim Güvenliği altyapısı mimarisi, sunucu altyapısı mimarisi ve yedeklilik yapısı bu şartname başlıklarına uygun bir şekilde YÜKLENİCİ tarafından hazırlanıp teklifle birlikte sunulacaktır.

### 2.4.2 Yüklenici Firma veya Altyüklenici Yetkinlikleri ve Detaylar

**2.4.2.1** Yüklenicinin ISO 9001:2015 Kalite Yönetim Sistemi sertifikası olmalıdır.

**2.4.2.2** Yüklenicinin ISO 20000-1:2011 Bilgi Teknolojileri Hizmet Yönetim Sistemi sertifikası olmalıdır.

**2.4.2.3** Yüklenicinin ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi sertifikası olmalıdır.

### 2.4.3 Yüklenici Veya Altyüklenici Firma Personel Yetkinlikleri ve Detaylar

**2.4.3.1** Yüklenicinin en az 1 adet Prince2 veya PMP eğitimi almış Proje yöneticisi olmalıdır.

**2.4.3.2** Yüklenicinin 1 adet teklif edilecek güvenlik duvarı ürününe ait uluslararası geçerliliği olan üretici tarafından verilmiş yetkinlik sertifikasına sahip personeli olmalıdır.

**2.4.3.3** Yüklenicinin 1 adet CCNP sertifikalı personeli olmalıdır.

**2.4.3.4** Yüklenicinin 1 adet MCSE sertifikalı personeli olmalıdır.

### 2.4.4 Referanslar ve Detaylar

**2.4.4.1** Tercihen finans kuruluşlarına yapılmış kapsamlı işlere ait iş bitirme belgeleri referans olarak sunulmalıdır.

## 2.5 VERİ MERKEZİ GENEL ŞARTLARI VE DETAYLARI

### 2.5.1 Detaylar

**2.5.1.1** İki ayrı Veri Merkezine (AKTİF DC ve PASİF DC), bu ihale kapsamında alınacak ürünlerin tamamı YÜKLENİCİ tarafından kurulacaktır.

**2.5.1.2** Tüm sunucular aynı marka olacaktır.

**2.5.1.3** Tüm ağ anahtarları aynı marka olacaktır.

**2.5.1.4** İDARE'nin mevcut sanal sunucuları Ortak Veri Merkezine taşınacaktır.

**2.5.1.5** Felaket anında Ana Veri Merkezindeki belirlenen sunucuların 30 dakika içerisinde FKM Veri Merkezinde çalışır durumda olması için gerekli altyapı kurulacaktır.

**2.5.1.6** Veri Merkezinde çift olarak konumlandırılacak cihazlar yedekli mimaride çalışmalıdır.

**2.5.1.7** Birbirinin yedeği olarak çalışacak tüm cihazlar Ana Veri Merkezi içinde farklı kabinetlerde konumlandırılacaktır. Kabinet içi cihaz montajları eksiksiz bir şekilde ve belirlenmiş standartlarda olacaktır.

**2.5.1.8** Her cihazın yedekli Güç Kaynakları Kabinet içinde bulunan ve yedekli çalışan Güç Dağıtım Birimlerine (PDU) bağlanacaktır. Tüm cihazların topraklama bağlantısı yapılmalıdır. Güç Dağıtım Birimlerinin yedekliği Veri Merkezi Sağlayıcısı tarafından karşılanacaktır.

**2.5.1.9** Cihazlar arasındaki tüm kablolama yedekli bir yapıda kurulacaktır. Kabinetler arası kablolama aynalama yöntemi ile yapılacaktır. Veri Merkezinde 2 kabin bulunacak, FKM'de 1 kabin bulunacaktır.

**2.5.1.10** Tüm cihazlar için güç, veri ve ağ bağlantı kablolarının her iki ucu da İDARE'nin belirleyeceği standartta etiketlendirilecektir.

**2.5.1.11** Veri Merkezinde konumlandırılacak Sunucuların 10GBps bağlantıları DataCenter Ağ Anahtarlarında, yönetim bağlantıları ise Yönetim Anahtarlarına yedekli bir şekilde bağlanacaktır.

**2.5.1.12** DataCenter Ağ Anahtarlar sanal şasi mimarisine göre yapılandırılarak tek bir anahtar gibi çalışması sağlanacaktır. DataCenter Ağ Anahtarları arası bağlantı en az 2 X 40GBps hızında olacaktır.

**2.5.1.13** Ana Veri Merkezinde konumlandırılacak ve aktif-aktif çalışacak yedekli Güvenlik Duvarlarının her bir Veri Merkezi Ağ Anahtarlarına en az 40 GBps hızında bağlanacaktır.

**2.5.1.14** Yüklenici her iki Veri Merkezinin çalışma şeklini detaylı çizim ve açıklamalarla dijital ortamda sunum ve rapor olarak İDARE'ye iletecektir.

**2.5.1.15** Bu ihale kapsamında temin edilecek tüm donanımsal ürünler için 5 (beş) yıl süreli, 7 gün 24 saat esasına dayalı garanti ve destek hizmeti sağlanacaktır.

## 2.6 VERİ MERKEZİ DONANIMLARI

### 2.6.1 Sunucu ve Depolama Sistemi Genel

**2.6.1.1** YÜKLENİCİ; Sunucu ve depolama sistemi yerine, Hiper Tümleşik (Hyper-converged Infrastructere) Altyapı önerebilir.

**2.6.1.2** Hiper Tümleşik (Hyper-converged Infrastructere) Altyapı önerilmesi durumunda önerilen sistem aşağıdaki şartları sağlayacaktır.

**2.6.1.2.1** Teklif edilecek bütünleşik sisteminin üreticisi, en son "Gartner Magic Quadrant for Hyperconverged Infrastructure" adlı değerlendirme raporunda Liderler (Leaders) konumunda olmalıdır veya yerli ürün olmalıdır.

**2.6.1.2.2** Önerilen sistemde Aktif DC tarafında minimum 7500GB, Pasif DC tarafında minimum 1500GB kullanılabilir bellek bulunacaktır.

**2.6.1.2.3** Önerilen sistem sıkıştırma öncesi Aktif DC tarafında minimum RAID6 yapilandirmasi sonrasi 200TB NVMe, Pasif DC tarafında minimum RAID6 yapilandirmasi sonrasi 150TB NVMe net kullanılabilir alana sahip olacaktır.

**2.6.1.2.4** Önerilen sistemin çalışabilmesi için gerekli tüm donanım (sunucu, switch vb) ve lisanslar verilecektir.

**2.6.1.2.5** Hiper Tümleşik (Hyper-converged Infrastructere) Altyapı önerilmesi durumunda Ek-2 malzeme listesi kullanılacaktır. Aksi takdirde Ek-1 malzeme listesi kullanılacaktır.

### 2.6.2 Fiziksel Sunucu – Aktif DC

**2.6.2.1** Teklif edilecek sunucu "rack" tipi olacaktır.

**2.6.2.2** Sunucunun merkezi işlem birimleri 64-bit mimaride çalışabilecektir.

**2.6.2.3** Teklif edilecek sunucu en az 2U yüksekliğe sahip olacaktır.

**2.6.2.4** Sunucu üzerinde en az 2 adet, temel çalışma frekansı en az 2 GHz olan, en az 3 UPI bağlantı sayısını destekleyen ve 16 GT/s UPI hızına sahip işlemciler bulunacaktır.

**2.6.2.5** Sunucu üzerindeki işlemcilerin her biri en az 24 adet çekirdeğe sahip olacaktır.

**2.6.2.6** Sunucu üzerindeki işlemcilerin her birinin üzerinde en az 45MB L3 cache belleği bulunacaktır.

**2.6.2.7** Sunucu üzerinde DDR5 tipinde, en az 4400MT/s hızında ve en az toplam 1536 GB kapasitede bellek bulunacaktır. Sunucu üzerinde bulunan bellek modülleri üretici tarafından onaylanmış bellekler olacaktır.

**2.6.2.8** Sunucu üzerinde en az 32 adet bellek yuvası bulunacaktır ve en az 4TB bellek kapasitesi desteklenecektir.

**2.6.2.9** Sunucu en az ECC veya Advanced ECC, Fast Fault Tolerance veya Adaptive Double Device Data Correction (ADDDC), SDDC, Memory Mirroring özelliklerini desteklemelidir.

**2.6.2.10** Sunucu en az 8 adet 2.5" disk takılabilecek şekilde teklif edilecek ve şasi SAS/SATA desteğine sahip olacaktır.

**2.6.2.11** Sunucu üzerinde, üzerinde en az 2 adet 480GB kapasitede NVMe veya M.2 SSD olan çalışma esnasında sökülüp takılabilen, RAID 1 yapısında olan kart olmalıdır.

**2.6.2.12** Sunucu üzerinde en az 2 adet 1Gbit RJ45 ethernet portu bulunmalıdır.

**2.6.2.13** Sunucu üzerinde en az 2 adet, OCP 3.0 mimarisinde, 10/25GbE fiber ethernet portu bulunmalıdır. Teklif edilecek bu ethernet kartı onboard olabilir. Portlar ile birlikte sunucu ile aynı marka orijinal 2 adet 25 Gbps hızında transceiver ve 5 (beş) metre uzunluğunda bağlantı kablosu eklenmelidir.

**2.6.2.14** Sunucu üzerinde en az 2 adet 1 Port 32G HBA kartlarla beraber aynı hızda transceiver ve OM4 tipinde 5 (beş) metrelik fiber kablo dahil edilmelidir.

**2.6.2.15** Teklif edilecek sunucu modeli SAS, NL-SAS, NL-SATA, U.2 NVMe PCIe SSD ve M.2 SSD disk tiplerini desteklemelidir.

**2.6.2.16** Teklif edilecek sunucu üzerinde uzaktan yönetim portu bulunmalıdır. Uzaktan yönetim portu ile sunucu uzaktan grafik arayüzü ile yönetilebilmelidir. Yönetim portu desteklediği en üst seviye lisanslarla birlikte teklif edilmelidir.

**2.6.2.17** Teklif edilecek sunucu 60Hz'de en az 1920x1200 çözünürlüğü destekleyen 16MB bellekli entegre veya kart şeklinde grafik işlemciye sahip olacaktır.

**2.6.2.18** Teklif edilecek sunuculardan 3 tanesine GPU kartı eklenecektir. GPU kartlar aşağıdaki özelliklere sahip olacak, GPU kartlar LLM amaçlı tekil bir sanal sunucu tarafından kullanılacak, üreticinin gerekliliği için ek bir lisans sağlanması gerekiyor ise bu lisans da birlikte sağlanacaktır.

**2.6.2.18.1** GPU Memory değeri en az 48 GB olacaktır.

**2.6.2.18.2** Memory Bandwith değeri en az 600 GB/sec olacaktır.

**2.6.2.18.3** Bfloat 16 performansı en az 145 TFLOPS olacaktır veya bu performansı karşılamayan üretici 2 kart olarak konumlandırılmalıdır.

**2.6.2.19** Teklif edilecek sunucu üzerinde, hot-swap ve redundant (yedekli) yapıda Power Supply ve soğutma fanları bulunacaktır. Power supply'lar en az 1800 Watt gücünde olacaktır.

**2.6.2.20** Teklif edilecek sunucu, üzerinde en az 4 (dört) adet fan barındıracaktır.

**2.6.2.21** Teklif edilecek sunucuda Trusted Platform Module (TPM) desteği bulunacaktır.

**2.6.2.22** Teklif edilecek sunucu üzerinde en az 4 (dört) adet PCI-Express 5.0 slotu desteği bulunacaktır.

**2.6.2.23** Teklif edilecek sunucuda en az 4 (dört) adet USB3.0 ve en az 1 (bir) adet VGA girişi bulunacaktır.

**2.6.2.24** Teklif edilecek sunucu üzerinde sistem durum bilgisini gösteren LED ışık göstergesi bulunacaktır.

**2.6.2.25** Sunucu üzerinde yetkisiz kişilerin disk değiştirmesini engellemek adına koruyucu, kilitlenebilir bezel bulunacaktır.

**2.6.2.26** Teklif edilecek sunucu üzerinde en az 2 adet GPU takılabilmesi desteklenmelidir.

**2.6.2.27** Teklif edilecek çözüm mimarisinin üreticiye ait sunucu yönetim yazılımı ve gerekli lisansları ile birlikte teklif edilmelidir. Yönetim modülü ile sunucunun uzaktan KVM (Keyboard, Video, Mouse) erişimi, uzaktan CD/DVD/Disk mount ederek işletim sistemi kurulum işlemi, güç tüketimi, sıcaklık, arıza izleme, donanım bileşenleri firmware güncelleme işlemleri yapılabilmelidir.

### 2.6.3 Fiziksel Sunucu – Pasif DC

**2.6.3.1** Teklif edilecek sunucu “rack” tipi olacaktır.

**2.6.3.2** Sunucunun merkezi işlem birimleri 64-bit mimaride çalışabilecektir

**2.6.3.3** Teklif edilecek sunucu en az 2U yüksekliğe sahip olacaktır.

**2.6.3.4** Sunucu üzerinde en az 2 adet, temel çalışma frekansı en az 2 GHz olan, en az 3 UPI bağlantı sayısını destekleyen ve 16 GT/s UPI hızına sahip işlemciler bulunacaktır.

**2.6.3.5** Sunucu üzerindeki işlemcilerin her biri en az 16 adet çekirdeğe sahip olacaktır.

**2.6.3.6** Sunucu üzerindeki işlemcilerin her birinin üzerinde en az 30MB L3 cache belleği bulunacaktır.

**2.6.3.7** Sunucu üzerinde DDR5 tipinde, en az 4400MT/s hızında ve en az toplam 768GB kapasitede bellek bulunacaktır. Sunucu üzerinde bulunan bellek modülleri üretici tarafından onaylanmış bellekler olacaktır.

**2.6.3.8** Sunucu üzerinde en az 32 adet bellek yuvası bulunacaktır ve en az 4TB bellek kapasitesi desteklenecektir.

**2.6.3.9** Sunucu en az ECC veya Advanced ECC, Fast Fault Tolerance veya Adaptive Double Device Data Correction (ADDDC), SDDC, Memory Mirroring özelliklerini desteklemelidir.

**2.6.3.10** Sunucu en az 8 adet 3.5” disk takılabilecek şekilde teklif edilecek ve şasi SAS/SATA desteğine sahip olacaktır.

**2.6.3.11** Sunucu üzerinde, üzerinde en az 2 adet 480GB kapasitede NVMe veya M.2 SSD olan çalışma esnasında sökülüp takılabilen, RAID 1 yapısında olan kart olmalıdır.

**2.6.3.12** Sunucu üzerinde en az 2 adet 1Gbit RJ45 ethernet portu bulunmalıdır. Teklif edilecek bu ethernet kartları onboard olabilir.

**2.6.3.13** Sunucu üzerinde en az 2 adet, OCP 3.0 mimarisinde, 25Gbps hızında fiber ethernet portu bulunmalıdır. Teklif edilecek bu ethernet kartı onboard olabilir. Portlar ile birlikte sunucu ile aynı marka orijinal 2 adet 25 Gbps hızında transceiver ve 5 (beş) metre uzunluğunda bağlantı kablosu eklenmelidir.

**2.6.3.14** Sunucu üzerinde en az 2 adet 1 Port 32G HBA kartlarla beraber aynı hızda transceiver ve OM4 tipinde 5 (beş) metrelik fiber kablo dahil edilmelidir.

**2.6.3.15** Teklif edilecek sunucu modeli SAS, NL-SAS, NL-SATA, U.2 NVMe PCIe SSD ve M.2 SSD disk tiplerini desteklemelidir.

**2.6.3.16** Teklif edilecek sunucu üzerinde uzaktan yönetim portu bulunmalıdır. Uzaktan yönetim portu ile sunucu uzaktan grafik arayüzü ile yönetilebilmelidir. Yönetim portu desteklediği en üst seviye lisanslarla birlikte teklif edilmelidir.

**2.6.3.17** Teklif edilecek sunucu 60Hz’de en az 1920x1200 çözünürlüğü destekleyen 16MB bellekli entegre veya kart şeklinde grafik işlemciye sahip olacaktır.

**2.6.3.18** Teklif edilecek sunucu üzerinde, hot-swap ve redundant (yedekli) yapıda Power Supply ve soğutma fanları bulunacaktır. Power supply’lar en az 1800 Watt gücünde olacaktır.

**2.6.3.19** Teklif edilecek sunucu üzerinde en az 4 (dört) adet fana sahip olmalıdır.

**2.6.3.20** Teklif edilecek sunucuda Trusted Platform Module (TPM) desteği bulunmalıdır.

**2.6.3.21** Teklif edilecek sunucu üzerinde en az 4 (dört) adet PCI-Express 5.0 slotu desteği bulunacaktır.

**2.6.3.22** Teklif edilecek sunucuda en az 4 (dört) adet USB3.0 ve en az 1 (bir) adet VGA girişi bulunacaktır.

**2.6.3.23** Teklif edilecek sunucu üzerinde sistem durum bilgisini gösteren LED ışık göstergesi bulunacaktır.

**2.6.3.24** Sunucu üzerinde yetkisiz kişilerin disk değiştirmesini engellemek adına koruyu, kilitlenebilir bezel bulunacaktır.

**2.6.3.25** Teklif edilecek çözüm mimarisinin üreticiye ait sunucu yönetim yazılımı ve gerekli lisansları ile birlikte teklif edilmelidir. Yönetim modülü ile sunucunun uzaktan KVM (Keyboard, Video, Mouse) erişimi, uzaktan CD/DVD/Disk mount ederek işletim sistemi kurulum işlemi, güç tüketimi, sıcaklık, arıza izleme, donanım bileşenleri firmware güncelleme işlemleri yapılabilmelidir.

### 2.6.4 Sunucu Depolama Ünitesi – Aktif DC

**2.6.4.1** Teklif edilen veri depolama sistemi kendi ürün ailesinin en son nesil ürünü olacaktır ve 2028 takvim yılı sonuna dek “End Of Life” ve “End Of Sale” duyurusu yapılmayacak olan bir ürün olacaktır.

**2.6.4.2** Veri Depolama Ünitesi üreticisi, son yayınlanan “Gartner Magic Quadrant for General-Purpose Disk Arrays” raporunda “Leaders” (liderler) konumunda veya yerli ürün olacaktır.

**2.6.4.3** Teklif edilen ürün SAN mimaride çalışacaktır. NAS mimarisi ile SAN opsiyonu sağlayan çözümler kabul edilmeyecektir.

**2.6.4.4** Tüm sistem komponentleri (disk kontrol üniteleri, güç üniteleri vb.) yedekli olmalıdır.

**2.6.4.5** Teklif edilen veri depolama sistemi içerisinde Intel/Amd/ARM işlemciler bulunmalıdır.

**2.6.4.6** Farklı marka disk sistemlerini tek bir veri havuzu gibi gösterebilecek veya gerektiğinde farklı marka disk sistemlerinden teklif edilecek veri depolama ünitesine veri aktarımı sağlanabilecektir. Bu işlem için gerekli olan lisanslar teklife dahil edilecektir. Bu özelliği desteklemeyen sistemler, teklif edilen her disk tipi için istenen brüt kapasitenin %20 fazlası ile teklif vereceklerdir. Bu ozellik kapsamında desteklenen marka/markalar teklifte belirtilecektir.

**2.6.4.7** Teklif edilen veri depolama sistemi en az 2 adet kontrol ünitesinden oluşmalıdır. Herhangi bir kontrol ünitesi bozulduğunda diğer kontrol ünitesi üzerinden veri depolama sistemi üzerindeki verilere ulaşım sağlanabilecektir.

**2.6.4.8** Teklif edilecek veri depolama sistemi 2 ayrı fiziksel lokasyonda çalışmayı desteklemelidir. Veri depolama ünitesi her iki lokasyona da aktif olarak yazmalı, cevap ihtiyaçlarını kendi lokasyonundaki veri depolama sisteminden almalıdır. Eğer bir lokasyondaki sistem kesintiye uğrarsa; herhangi bir fiziksel müdahaleye gerek duymadan, diğer lokasyondaki sistem üzerinden kesintisiz olarak hizmet vermeye devam edebilecektir. Bu kontrol üniteleri aktif/aktif çalışabilecek, herhangi bir kontrol ünitesi bozulduğunda diğer kontrol ünitesi üzerinden veri depolama sistemi üzerindeki verilere ulaşım sağlanabilecektir. Bu özellik ek donanımlar ile sağlanıyorsa ek donanımlar, garantileri ve lisansları teklife dahil edilmelidir.

**2.6.4.9** Teklif edilen her bir veri depolama sistemi üzerlerinde bulunan her bir kontrol ünitesi üzerinde blok erişim için en az 256 GB olmak üzere, toplamda en az 512GB önbelleğe sahip olmalıdır.

**2.6.4.10** Flash disklerden oluşturulmuş ve disk tabanlı ön bellek mimarisi kabul edilmeyecektir.

**2.6.4.11** Teklif edilen veri depolama sistemi üzerinde her bir kontrol (controller) ünitesinde en az 16 çekirdekli işlemci olacaktır.

**2.6.4.12** Teklif edilen veri depolama sistemi tek bir veri depolama ünitesi üzerinde 24 adet SCM desteklemeli veya bu özellik desteklenmiyorsa kontrol ünitesi değişikliğine ve eklentisine gitmeden en az 72 adet NVMe’ye genişleyebilen bir veri depolama ünitesi teklif edilmelidir.

**2.6.4.13** Teklif edilen veri depolama sistemi üzerindeki disk yuvalarının tamamı uçtan uca NVME protokolünü desteklemelidir.

**2.6.4.14** Teklif edilen veri depolama sistemi 1.92TB, 3.84TB, 7.68TB, 15.36TB NVMe SSD sürücüleri desteklemelidir veya 4.8TB, 9.6TB, 19.2TB, 38.4TB NVMe modülleri desteklemelidir.

**2.6.4.15** Teklif edilecek veri depolama sistemi üzerinde NVMe sürücüler kullanılarak raid6 veya muadili bir koruma yapılandırması kullanılarak 200 TB net kullanılabilir alan sağlanmalıdır.

**2.6.4.16** Teklif edilecek veri depolama sistemi üzerinde oluşabilecek disk arızalarına karşı üzerinde bulunan her bir disk tipi için (NVMe, SCM, FCM, Flash Drive, SSD) veri depolama sisteminde yedek (hotspare) disk teklif edilecek ve bu disk otomatik olarak sistem içerisinde yer alan ve arızalanan herhangi bir disk yerine geçecektir. Sistem yedek disk alanını kullanılmakta olan disklere dağıtarak sağlıyorsa, bu alan teklif edilen her 24 disk için bir disk alanı kadar yedek alan şeklinde tekliflendirilecek, bu yedek alan kullanılabilir alan hesaplamalarına dâhil edilmeyecektir.

**2.6.4.17** Teklif edilen veri depolama ünitesi üzerinde tanımlanabilen ve atanabilen mantıksal disk (LUN) adedi, kullanımında herhangi bir kısıtlama olmaksızın en az 4096 (dört bin doksan altı) adet olacaktır. Sistem en az 64 TiB büyüklüğünde mantıksal alan (LUN) yaratabilme özelliğine sahip olmalıdır. Sistemler maksimum LUN sayısını desteleyecek şekilde teklif edilecektir.

**2.6.4.18** Veri depolama sisteminin sunuculara olan bağlantısını sağlamak amacıyla; teklif edilen veri depolama sistemi üzerinde bulunan kontrol ünitelerinin her biri üzerinde 4 adet olmak üzere toplamda en az 8 adet 32 Gbps bağlantı hızını destekleyen FC portlar ve toplam en az 4 adet 10 Gbps bağlantı hızını destekleyen iSCSi portlar bulunmalıdır. Teklif edilen veri depolama sistemi üzerindeki bütün sunucu bağlantı noktaları, portlardaki en yüksek hız değerini destekleyecek nitelikte en az 5 (beş) metre uzunluğunda bağlantı kabloları ile takılı olarak teslim edilecektir.

**2.6.4.19** Teklif edilen veri depolama sistemi %70 okuma, %30 yazma, 8K blok boyutu, 180.000 IOPS değerini 1ms altında verebilmelidir.

**2.6.4.20** Teklif edilen veri depolama sistemi yazılan verinin erişebilirliğini sağlayacak koruma teknolojisine sahip olacaktır. Veri depolama sistemi veriyi dağıtarak yazan Distributed RAID 1 ve/veya RAID 6 koruma yöntemlerini destekleyecektir.

**2.6.4.21** Teklif edilen veri depolama sistemi, üzerinde bulunan verilerin anlık kopyalarını alabilme ve alınan verinin geri dönülmesi özelliğine sahip olmalıdır (Snapshot ve Clone). Bu işlem için gerekli olan yazılımlar ve lisanslar teklif edilen net kapasite kadar verilecektir.

**2.6.4.22** Teklif edilen veri depolama sistemi üzerinde, belirlenen kurallar çerçevesinde, silinemez ve değiştirilemez snapshotlar alınabilmelidir. Bu özellik sağlanmıyorsa kullanılan disk tipleriyle aynı olmak kaydıyla en az %30 daha fazla ham kapasite sağlamalıdır.

**2.6.4.23** Teklif edilen veri depolama sistemi, uzak noktada bulunan eş özelliklere sahip olan veri depolama sistemine senkron ve asenkron olarak veri replikasyonunu native olarak desteklemelidir. Bu iş için gerekli olan yazılımlar ve lisanslar teklif edilen net kapasite kadar verilecektir.

**2.6.4.24** Teklif edilen veri depolama sistemi “Thin Provisioning” özelliğine sahip olmalıdır. Bu işlem için gerekli olan yazılımlar ve lisanslar teklif edilen net kapasite kadar verilecektir.

**2.6.4.25** Teklif edilen harici veri depolama birimi blok seviyesinde anlık (inline) sıkıştırma (compression) / anlık (inline) tekilleştirme (deduplication) veya anlık (inline) zero detection gibi alan tasarrufu sağlayacak teknolojilerden en az birine sahip olmalıdır. Bu özellik desteklenen maksimum sayıda disk veya disk alanı için teklife dahil edilmelidir.

**2.6.4.26** Sıkıştırma veya tekilleştirma teknolojisi teklif edilen bütün disk tiplerinde kullanılabilir olmalıdır. Sıkıştırma ve tekilleştirme desteklenmeyen disk tipleri (NVMe Flash, SSD) için teklif edilen brüt kapasitesinin %30’u kadar ek kapasite teklife eklenmelidir.

**2.6.4.27** Sistemin yönetim yazılımı üzerinde olacaktır. Yönetim için CLI ve GUI arayüzü bulunacaktır.

**2.6.4.28** Teklif edilen veri depolama sistemi, Windows, Linux vb. gibi güncel işletim sistemleri ve Vmware sanallaştırma sistemine uyumlu olmalıdır.

### 2.6.5 Sunucu Depolama Ünitesi – Pasif DC

**2.6.5.1** Teklif edilecek harici veri depolama sistemi, birden fazla veri depolama sisteminin kümeleme veya benzeri yöntemlerle birleştirilmesinden oluşmuş olmamalıdır.

**2.6.5.2** Teklif edilecek harici veri depolama sisteminin üreticisi, son yayınlanan "Gartner Magic Quadrant for General-Purpose Disk Arrays" adlı değerlendirme raporunda Liderler (Leaders) konumunda olmalıdır veya yerli ürün olmalıdır.

**2.6.5.3** Teklif edilecek harici veri depolama sisteminde tek noktadan hata durumuna karşı önlemler alınmış olmalı ve herhangi bir parçanın arızasında yedek birim veri depolama sisteminin durmadan çalışmasını sağlamalıdır.

**2.6.5.4** Teklif edilecek harici veri depolama sisteminde denetleme birimi kod güncellemeleri ve arıza durumunda parçaların (disk, güç kaynağı, fanlar, vs.) değiştirilmesi sistem çalışırken yapılabilmelidir.

**2.6.5.5** Teklif edilecek harici veri depolama sistemi üzerinde en az 24 GB DRAM tabanlı önbellek bulunmalıdır.

**2.6.5.6** Veri depolama sistemi FC, iSCSI veya SAS protokollerini sunucu bağlantıları için, ek ara katman (gateway) veya lisans gereksinimi olmadan desteklemelidir.

**2.6.5.7** Teklif edilen veri depolama sistemini disk çekmecelerine bağlantı arayüzü 12Gbps SAS olmalıdır.

**2.6.5.8** Teklif edilecek veri depolama sistemi üzerinde en az 17 adet her biri en az 3.84TB Flash Drive olmalıdır.

**2.6.5.9** Teklif edilecek veri depolama sistemi, RAID10 (veya 1/0), RAID5 ve RAID6 koruma seviyelerini desteklemelidir. Alternatif veri koruma yöntemleri kabul edilmeyecektir.

**2.6.5.10** Teklif edilecek veri depolama sistemi 2.5" veya 3.5" boyutunda en az 240 adet disk takılmasını desteklemelidir. Desteklenen disk tipleri arasında SSD, SAS, NL-SAS, MDL-SAS veya bunların SED seçenekleri olmalıdır.

**2.6.5.11** Teklif edilecek veri depolama sistemi en az 2 PB brüt kapasiteyi desteklemelidir.

**2.6.5.12** Teklif edilecek veri depolama sistemi kabinet birimi (rack unit) başına en az 150TB ham kapasite sağlayabilen çekmece desteği bulunmalıdır.

**2.6.5.13** Teklif edilecek veri depolama sistemi, istendiği takdirde sisteme eklenebilecek SSD'lerin önbellek olarak kullanımını desteklemelidir. SSD önbellek kapasitesi 4TB'a kadar yükseltilebilmelidir. Bu özellik için ek bir lisans gereksinimi olmayacaktır."

**2.6.5.14** Teklif edilecek harici veri depolama sisteminde en az 8 adet, her biri en az 16 Gbps bant genişliğini destekleyen ve fiber kanal bağlantıya imkân tanıyan sunucu bağlantı portu olacaktır. Bu portlar için, en yüksek hız değerini destekleyecek şekilde en az 5 (beş) metre uzunluğunda OM4 tipinde fiber optik bağlantı kabloları sağlanacaktır.

**2.6.5.15** Teklif edilecek harici veri depolama sistemi asenkron, replikasyonu desteklemelidir. Bu özellik için ek donanım ve lisans gerekiyorsa teklife maksimum kapasite için eklenmelidir.

**2.6.5.16** Teklif edilecek harici veri depolama sistemi snapshot (anlık kopya) ve tam kopya (clone/volume copy) alabilmeli ve bu kopyalardan geri dönebilmelidir (restore/rollback). Bu özellik için gerekli lisanslar sistemin desteklediği maksimum kapasite için teklife eklenecektir.

**2.6.5.17** Teklif edilecek harici veri depolama sistemi thin provisioning özelliğine sahip olacaktır. Bu özellik için gerekli lisanslar şartnamede istenen kapasite için teklife eklenecektir.

**2.6.5.18** Teklif edilecek harici veri depolama sistemiyle birlikte grafik arayüzlü yönetim yazılımı sağlanacaktır. Yönetim yazılımı ile sistem alarmları, boş alan, kapasite bilgileri, donanım durumları, LUN yapılandırmaları vb. durum bilgileri gözlemlenebilecektir.

**2.6.5.19** Sistemde kullanılmakta olan sanal disk gruplarının en az 1 çeşidi kapsamında erişim kesintisi olmadan ilaveler yapılabilmelidir.

**2.6.5.20** Teklif edilecek veri depolama sisteminde, en az 64TiB kapasitesinde mantıksal alanlar (LUN) oluşturulabilmelidir.

**2.6.5.21** Teklif edilen veri depolama ünitesinde en az 512 (beşyüzoniki) LUN oluşturulabilmelidir.

**2.6.5.22** Teklif edilecek harici veri depolama sistemi, üzerinde oluşan bir arıza durumunda sistem yöneticisini e-posta ile uyarma özelliğine sahip olacaktır.

**2.6.5.23 Teklif edilecek harici veri depolama sisteminin 5 yıl, 7/24, destek ertesi iş günü yerinde müdahale kapsamında üretici firma garantisi olacaktır.**

### 2.6.6 SAN Switch – Aktif DC

**2.6.6.1** SAN anahtarı 16 ve 32 Gbit/s hızını desteklemelidir.

**2.6.6.2** SAN anahtarları üzerindeki port sayısı 24 porta kadar çıkabilmelidir.

**2.6.6.3** SAN anahtarı üzerinde her biri 32Gbps hızında en az 16 port aktif olarak gelmelidir. SAN üzerindeki tüm portların bağlantı transceiver ve OM4 tipinde 5mtlik fiber optik kabloları sağlanmlıdır.

**2.6.6.4** SAN anahtarlar portlar arasinda local anahtarlama yapabilmelidir. (Local Switching)

**2.6.6.5** SAN anahtarı NVMe-Ready olmalıdır.

**2.6.6.6** Desteklenen frame Base ISL Trunking'i desteklemelidir.

**2.6.6.7** Desteklenen frame Base Trunking hızı en az 256 Gbps olmalıdır.

**2.6.6.8** San anahtarı, E, F, M, ve D port tiplerini desteklemelidir.

**2.6.6.9** Ürünlerin desteği ve kurulum hizmeti OEM'leyen depolama sistem üretici tarafından verilecektir.

### 2.6.7 Veri Merkezi Ağ Anahtarı – Aktif DC

**2.6.7.1** Tekli Minimum 48 adet GE/10GE/25GE SFP28 portuna sahip olmalıdır.

**2.6.7.2** Minimum 4 adet 40GE/100GE QSFP+/QSFP28 portuna sahip olmalıdır.

**2.6.7.3** Anahtarlar için toplam 8 adet 100Gbps QSFP, 28Adet 25Gbps SFP28, 2adet 10Gbps SFP+ orijinal transceiver ve 5mt uzunluğunda bağlantı kabloları sağlanmalıdır.

**2.6.7.4** Minimum 1 adet RJ-45 Seri Konsol portuna sahip olmalıdır.

**2.6.7.5** STP Protokolünü desteklemelidir. Aynı zamanda STP'nin uzantıları olan BPDU Koruması, Loop Koruması gibi teknolojileri de desteklemeldir.

**2.6.7.6** Cihaz tıkanmasız bir şekilde L2/L3 operasyonlarını yapabilmelidir.

**2.6.7.7** Minimum 64K MAC adresi desteklemelidir.

**2.6.7.8** Minimum 2000 Mpps paketi anahtarlayabilmelidir.

**2.6.7.9** Minimum 3200 Gbps anahtarlama kapasitesine sahip olmalıdır.

**2.6.7.10** Cihazın latency değeri 1 mikro saniyenin altında olmalıdır.

**2.6.7.11 Özelliklerin aktif olarak çalıştırılması için lisans gerekiyorsa, sağlanacak tüm lisansların geçerlilik süresi en az 5 yıl olmalıdır.**

**2.6.7.12** Sistem odası ortamı ısı ve nem oranları standartlarında, %15 den %90 a kadar olan nem ortamında ve 0°C to +40°C sıcaklık aralığında çalışabilmelidir.

**2.6.7.13** Anahtar cihaz yönetim protokolü olarak TACACS+ (RFC 1492) desteklemelidir.

### 2.6.8 Veri Merkezi Ağ Anahtarı – Pasif DC

**2.6.8.1** Tekli Minimum 48 adet GE/10GE/25GE SFP28 portuna sahip olmalıdır.

**2.6.8.2** Minimum 4 adet 40GE/100GE QSFP+/QSFP28 portuna sahip olmalıdır.

**2.6.8.3** Anahtarlar için toplam 8 adet 100Gbps QSFP, 28Adet 25Gbps SFP28, 2adet 10Gbps SFP+ orijinal transceiver ve 5mt uzunluğunda bağlantı kabloları sağlanmalıdır.

**2.6.8.4** Minimum 1 adet RJ-45 Seri Konsol portuna sahip olmalıdır.

**2.6.8.5** STP Protokolünü desteklemelidir. Aynı zamanda STP'nin uzantıları olan BPDU Koruması, Loop Koruması gibi teknolojileri de desteklemeldir.

**2.6.8.6** Cihaz tıkanmasız bir şekilde L2/L3 operasyonlarını yapabilmelidir.

**2.6.8.7** Minimum 64K MAC adresi desteklemelidir.

**2.6.8.8** Minimum 2000 Mpps paketi anahtarlayabilmelidir.

**2.6.8.9** Minimum 3200 Gbps anahtarlama kapasitesine sahip olmalıdır.

**2.6.8.10** Cihazın latency değeri 1 mikro saniyenin altında olmalıdır.

**2.6.8.11 Özelliklerin aktif olarak çalıştırılması için lisans gerekiyorsa, sağlanacak tüm lisansların geçerlilik süresi en az 5 yıl olmalıdır.**

**2.6.8.12** Sistem odası ortamı ısı ve nem oranları standartlarında, %15 den %90 a kadar olan nem ortamında ve 0°C to +40°C sıcaklık aralığında çalışabilmelidir.

**2.6.8.13** Anahtar cihaz yönetim protokolü olarak TACACS+ (RFC 1492) desteklemelidir.

### 2.6.9 Yönetim Anahtarı – Aktif DC/ Pasif DC

**2.6.9.1** Minimum 48 Port 1G Copper cihaz olmalıdır ve portların hepsi aynı anda kullanılabilecektir.

**2.6.9.2** Minimum 2 adet 10G uyumlu fiber porta sahip olmalıdır, üzerindeki tüm portlar multi-mode fiber destekleyecek 10G SFP+ modüller ile tekliflendirilmelidir.

**2.6.9.3** Cihaz tıkanmasız bir şekilde L2/L3 operasyonlarını yapabilmelidir.

**2.6.9.4** Sağlanacak tüm anahtarlar için toplam 3 adet 10Gbps SFTP+ transceiver ve 5 (beş) metre uzunluğunda bağlantı kabloları ile 40 adet 5mt UTP Cat6 bakır kablo temin edilmelidir.

**2.6.9.5** Minimum 24K MAC adresi desteklemelidir.

**2.6.9.6** Minimum 80 Mpps paketi anahtarlayabilmelidir.

**2.6.9.7** Minimum 136 Gbps anahtarlama kapasitesine sahip olmalıdır.

**2.6.9.8 Özelliklerin aktif olarak çalıştırılması için lisans gerekiyorsa, sağlanacak tüm lisansların geçerlilik süresi en az 5 yıl olmalıdır.**

**2.6.9.9** Sistem odası ortamı ısı ve nem oranları standartlarında, %15 den %90 a kadar olan nem ortamında ve 0°C to +40°C sıcaklık aralığında çalışabilmelidir.

**2.6.9.10** Anahtar cihaz yönetim protokolü olarak TACACS+ (RFC 1492) desteklemelidir.

### 2.6.10 Güvenlik Duvarı – Aktif DC

**2.6.10.1** Güvenlik duvarı yedekli HA çifti şeklinde teklif edilecektir. Buna göre aynı veri merkezinde aktif cihazda bir sorun olması durumunda; tüm trafik otomatik olarak aynı veri merkezinde konumlanmış pasif cihaza aktarılacaktır. Bu durumda uygulama tanıma ve routing özellikleri pasif cihaz üzerinden bir kesinti olmadan çalışacaktır.

**2.6.10.2** Ağ Cihazı, mimari açıdan stateful inspection, IP Paket Filtreleme ve Uygulama Tanıma özelliklerini bünyesinde bulundurmalı ve aşağıdaki güvenlik servislerine sahip olmalıdır. Anti-Virus, DNS Security, URL Filtreleme ve Sıfırıncı Gün Koruma tarafında gelişmiş özelliklerin tümünün kullanılabilmesi için gerekli tüm lisanslar teklife eklenmelidir.

I. Firewall
II. IPSEC VPN, SSL VPN
III. Uygulama kontrolü (Application Control)
IV. Atak Engelleme (IPS)
V. Anti-Virus
VI. Anti-Spyware/Anti-Bot
VII. URL Filtreleme
VIII. DNS Security
IX. Kullanıcı kimliği entegrasyon
X. SSL Inspection
XI. Sıfırıncı gün koruma (cloud sandbox desteği)

**2.6.10.3** Teklif edilecek olan her iki sistem port ve performans anlamında birbiriyle aynı marka model ve kapasitede olmalıdır.

**2.6.10.4** Uzun süreli kullanım açısından (End-of-Order, End-of-Sale) teklif edilecek güvenlik duvarı donanım modelinin piyasaya ilk çıkış tarihi belirtilmelidir. Daha yeni olan modeller tercih sebebi olacaktır.

**2.6.10.5** Ürün, yüksek performans ve düşük gecikme ihtiyacı nedeniyle ASIC veya FPGA veya integrated crypto assistant veya İntel tabanlı işlemci mimarisine sahip olması tercih sebebidir. Bu sayede özellikle SSL Deep Inspection gibi yüksek performans gereksinimi duyulan durumlarda performans sorunu yaşanmamalıdır.

**2.6.10.6** Ürün, aşağıda detayları belirtilen OSI mimarisine uygun çok katmanlı güvenlik modeline sahip olmalıdır.

**2.6.10.6.1** Güvenlik politikaları özelinde OSI L4 ve L7 katmanları arasında çalışabilmelidir. Bu sayede istenen trafikler L4 (kaynak ip/kullanıcı, hedef ip, hedef port) istenen trafikler L7 uygulama seviyesinde analiz edilebilmelidir.

**2.6.10.6.2** 7. katmanda uygulama seviyesinde analiz edilmesi gerekmeyen trafikler tipleri için (yedekleme trafiği, database senkronizasyonu v.b.) sistemin gereksiz yere performans tüketmesi engellenebilmeli ve sistem verimliliği arttırılabilmelidir.

**2.6.10.7** Politika özelinde L7 güvenlik servisleri aktif edilebilmelidir. Bu kapsamda aşağıda listelenen güvenlik servisleri tercihe bağlı olarak seçilebilmelidir.

I. Uygulama Kontrolü
II. Atak Engelleme (IPS)
III. AntiVirus, AntiMalware, Anti-Spyware/Anti-Bot
IV. URL/Web Filtreleme
V. DNS Security
VI. Dosya Filtreleme
VII. SSL Inspection

**2.6.10.8** Teklif edilen güvenlik duvarının firewall throughput değeri 70 (yetmiş) Gbps performansını desteklemelidir. Üreticinin herkese açık dökümanlarında bu değer açıkça belirtilmiş olmalıdır.

**2.6.10.9** Ürün, en az 15 (onbeş) Gbps tehdit engelleme (Firewall, Uygulama Kontrol, IPS, AntiMalware servisleri aktif) performans (throughput) değerine sahip olmalıdır. Üreticinin resmi web sayfasında ilgili değerin herkese açık bir şekilde yayınlanmış olması gerekmektedir.

**2.6.10.10** Ürün en az 28 (yirmisekiz) Gpbs IPSEC VPN performans değerine sahip olmalıdır.

**2.6.10.11** Ürün, aynı anda en az 7 (yedi) milyon oturumu desteklemelidir.

**2.6.10.12** Ürün, saniyede en az 370.000 (üçyüzyetmişbin) yeni oturum açabilme kapasitesine sahip olmalıdır.

**2.6.10.13** Ürün, aynı anda en az 4 adet 25GE SFP28 ve en az 2 adet 40G/100G QSFP/QSFP28, en az 4 adet 25GE veya 2 adet 10GE SFP+ fiber ve en az 6 adet 1 GE SFP bağlantı desteğine sahip olmalıdır. 10 GE port adetinin sayıca fazla olması ve 10 GE portların 25GE olarak kullanılabilir olması tercih sebebidir. Port "interface" sayıları dinamik "değiştirilebilir" olan üreticiler tüm ethernet kartlarının dolu olacağı max konfigürasyonu önermelidir.

**2.6.10.14** Cihazlar üzerinde en az ikişer adet 100Gbps QSFP, ikişer adet 1Gbps bakır, beşer adet 25GBps SFP28 orijinal transceiver ve bağlantı kablosu ile çalışır durumda olmalıdır.

**2.6.10.15** Şartnamede istenen performans ve port değerleri tek bir donanım ile karşılanamaması durumunda üretici firma birebir aynı özelliklere sahip donanım veya şase ürününden birden fazla teklif ederek isterleri kümeleme (clustering) ile sağlayabilecektir. Bu durumda cihazların isterlere uygun çalışabilmesi için gerekli cihaz ve yazılımlar da teklife dahil edilecektir. Kümeleme (clustering) yapılacak cihazların hepsi port ve performans anlamında birbiriyle aynı marka model ve kapasitede olmalıdır.

**2.6.10.16** Kurum kaynaklarına uzaktan güvenli erişiminin sağlanabilmesi için cihaz üzerinde aşağıda detayları belirtilen SSL-VPN özelliği olmalıdır.

**2.6.10.17** Cihaz aynı anda en az 2.000 (iki bin) kullanıcının SSL VPN ile bağlantısına izin verebilecek kapasitede olmalıdır.

**2.6.10.18** SSL VPN özelliği en az Windows, MAC OS, Linux, IOS ve Android işletim sistemlerini desteklemelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

**2.6.10.19** Farklı kullanıcılara farklı ip adresleri atanmasını desteklemelidir.

**2.6.10.20** SSL VPN üzerinden erişen kullanıcıların lokal kullanıcı veritabanı, RADIUS, LDAP veya Microsoft AD üzerinden kimlikleri doğrulanabilmelidir.

**2.6.10.21** SSL VPN tüneli içerisinden gelen trafiklerde IPS, Uygulama Kontrolü, AntiMalware, URL Filtreleme özellikleri uygulanabilir olmalıdır.

**2.6.10.22** SSL-VPN ile bağlantı yapacak adresler belirtilebilmeli, belirtilen adresler dışından SSL-VPN erişimleri engellenebilmelidir.

**2.6.10.23** Split tunnelling özelliği ile sadece belirtilen hedef adresler için trafiğin tünele yönlendirilmesi sağlanabilmelidir.

**2.6.10.24** DNS servisi için ayrıca split tunneling'i desteklemelidir. Bu sayede sadece spesifik domain sorguları için merkezdeki DNS sunucularının kullanımı sağlanabilmelidir.

**2.6.10.25** SSL-VPN ile bağlanacak kullanıcılar için two factor authentication (2FA) özelliği desteklenmelidir.

**2.6.10.26** SSL-VPN ile yapılan aktif bağlantılar monitör edilmelidir. Bağlı olan kullanıcı ve ne zaman login olduğu bilgilerine web tabanlı arayüz veya üreticinin kendi uygulaması üzerinden erişilebilmelidir.

**2.6.10.27** SSL-VPN portal özelliği ile son kullanıcı bilgisayarlarına yazılım (vpn agent) kurmadan portal üzerinden SSL VPN yapılabilmelidir. Portal üzerinden asgari HTTP(S), FTP, sFTP, VNC, RDP ve SSH uygulama ve protokol erişimleri desteklenmelidir.

**2.6.10.28** Firewall üzerinde en az 15 (on) adet sanal firewall oluşturulabilecek lisans ile teklif edilecektir. Sanal firewall sayısı 25'e kadar çıkartılabilmelidir.

**2.6.10.29** Her bir veri merkezi için güvenlik duvarı sistemi yedekli mimaride ikişer adet teklif edilecektir.

**2.6.10.30** Ürün, aktif-aktif ve aktif-pasif yedeklilik senaryolarını desteklemelidir.

**2.6.10.31** Kümeleme yapılan donanımlarda oturumlar donanımın herhangi birisinin arızalanması durumunda oturum kaybı olmadan otomatik olarak diğer güvenlik duvarı cihazı üzerinde devam edebilmelidir.

**2.6.10.32** Network arayüzlerinin herbiri LAN, WAN, DMZ veya kullanıcı tanımlı bir segment olarak konfigüre edilebilmelidir. İlgili arayüzler 802.1q protokolünü desteklemelidir. Her bir interface için Alias tanımı girilebilmelidir.

**2.6.10.33** Saat, gün bazında erişim kontrolü yapabilmelidir.

**2.6.10.34** Yerel ağdaki bir ya da birden fazla adres aralığındaki birçok IP'yi istenirse tek bir adres arkasında, istenirse her bir aralığı başka bir tek adres arkasında saklayabilmeli ya da bire bir adres çevrim özelliği (NAT) olmalıdır.

**2.6.10.35** NAT kuralları, Güvenlik kurallarından bağımsız ayrı kural seti olarak tanımlanabilecektir.

**2.6.10.36** DHCP server ve IPv4/v6 DHCP Relay olarak yapılandırabilecektir.

**2.6.10.37** Tek VLAN üzerinde en az 1000 adet, sanal firewall kullanıldığında ise toplamda en az 4000 adet VLAN desteği sağlamalıdır.

**2.6.10.38** Güvenlik Duvarı 802.3 ad LACP desteklemelidir.

**2.6.10.39** Güvenlik Duvarı SNMP v3 desteklemelidir.

**2.6.10.40** Güvenlik Duvarının Netflow desteği olmalıdır.

**2.6.10.41** Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dâhil edilmelidir.

**2.6.10.42** Yönetim arayüzü veya CLI üzerinden her bir fiziksel, interface için trafik kullanım değerleri gerçek zamanlı ve geçmişe dönük görüntülenebilmelidir. Bu sayede hangi interface üzerinde o an için ne kadar trafik kullanımı olduğu bilgisi (throughput) IN ve OUT yönlü analiz edilebilmelidir.

**2.6.10.43** Sistemin SPI (Stateful Packet Inspection) özelliği olmalıdır.

**2.6.10.44** RIP, OSPF, BGP, static ve kaynak tabanlı (policy based) yönlendirme özelliklerine sahip olmalıdır. Multicast routing'i desteklemelidir.

**2.6.10.45** Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dâhil edilmelidir.

**2.6.10.46** Path monitoring vb özelliği cihaz üzerinde tanımlanan statik route tanımları bağdaştırılabilecektir. Böylece tanımlanan statik yönlendirmeler üzerinden sağlanan erişimlerin çalışıp çalışmadığını kontrol edebilecektir. Erişim olmadığı durumlarda statik yönlendirme satırını yönlendirme tablosundan otomatik olarak kaldırarak alternatif yoldan erişim imkânı sağlanacaktır.

**2.6.10.47** Cihazın Multicast yönlendirme desteği olmalı ve PIM-SM, PIM-SSM, IGMP v1, v2, v3 desteklemelidir.

**2.6.10.48** Site to site ve client to site IPSEC VPN desteği olmalıdır.

**2.6.10.49** Cihaz, IPSec VPN standardını desteklemelidir. IKE şifreleme şemalarını desteklemelidir. 3DES, AES algoritmaları ile paket şifreleme yapabilmelidir. Veri bütünlüğü için MD5 ve SHA1 algoritmalarını desteklemelidir. Diffie-Hellman groups 1, 2 ve 5 (Perfect forward secrecy) desteği olmalıdır.

**2.6.10.50** Cihaz GRE tunnel destekleyecektir.

**2.6.10.51** Cihaz IPv6 IPsec destekleyecektir.

**2.6.10.52** DHCP Server ve DHCP Relay özelliği bulunmalıdır.

**2.6.10.53** NAT64 ve Jumbo frame desteği olmalıdır.

**2.6.10.54** Cihaz üzerindeki portlar Layer3 (routing mod) ve Layer2 (bridge mod) ve Monitoring (TAP mod) katmanlarında çalışabilecektir.

**2.6.10.55** Cihazın yeniden başlatılmasına gerek kalmadan üzerindeki portların çalışma seviyesi (L2, L3, monitoring) istendiği gibi değiştirilebilmelidir.

**2.6.10.56** Ağ arayüzü veya zone bazlı kural yazılmasını desteklemelidir.

**2.6.10.57** Saat, gün, tarih bazında erişim kontrolü yapabilmelidir.

**2.6.10.58** MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılabilecektir. Kullanıcıya göre kural yazma sadece kimlik bilgisi gönderen uygulamalarla sınırlı olmayacaktır. Tutulan kayıtlarda kullanıcı ismi de yer alacaktır.

**2.6.10.59** Kullanıcı entegrasyonu için yönetici (administrator) hesabına ve Active Directory yapısında herhangi bir değişikliğe ihtiyaç olmayacaktır.

**2.6.10.60** Cihaz kendisine kullanıcı doğrulaması yapan sistemlerin gönderdiği syslog veya benzeri mesajları çözerek User-IP mapping işlemini gerçekleştirebilecektir.

**2.6.10.61** Cihaz aynı anda farklı yöntemleri kullanarak farklı kaynaklardan IP-Kullanıcı eşleşmesini sağlayabilecektir.

**2.6.10.62** Kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS, LDAP ve AD üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

**2.6.10.63** Kullanıcı/kullanıcı grubu, kaynak ip/ağ, hedef ip/ağ ve uygulama bazlı bantgenişliği yönetim (QoS) desteği olmalıdır. Grup bazlı ya da uç nokta bazlı QoS yapılabilmelidir. QoS trafik için upload veya download yönünde ve zamana bağlı olarak hat kapasitesinin yüzdesel oranında veya bant genişliği kapasitesine göre tanımlanabilmelidir. Ses/video gibi kritik uygulamalara öncelik (priority) ve garanti bantgenişliği yazılabilmelidir. Belirlenen trafik için maksimum bantgenişliği tanımlama imkânı olmalıdır.

**2.6.10.64** SSL inspection (https trafiğinin açılması) desteği olmalıdır. Bu sayede ssl trafiklerini açarak, uygulama detaylarına göre; QoS, uygulama kuralları yazılabilmelidir.

**2.6.10.65** Sistem üzerinde detayları aşağıda belirtilen uygulama kontrol özelliği bulunmalıdır.

**2.6.10.66** Sistemin uygulama kütüphanesinde en az 2500 (iki bin beş yüz) adet uygulama yer almalıdır.

**2.6.10.67** Uygulama kütüphanesinde yer alan tüm uygulamalar aşağıda belirtilen parametrelere göre kategorize edilmiş olmalıdır.

**2.6.10.67.1** Uygulama davranışına göre (botnet, tünelleme amaçlı, bulut uygulaması, bandwith tüketim odaklı v.b.)

**2.6.10.67.2** Risk seviyesine göre (Critical, High, Medium, Low v.b.)

**2.6.10.67.3** Erişim yöntemine göre (Client-server, browser tabanlı, P2P gibi)

**2.6.10.68** Uygulama kontrol özelliği active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında uygulama kontrol kuralları tanımlanabilecektir.

**2.6.10.69** Veri tabanında yer alan uygulamaların listesi, ilgili uygulamanın yer aldığı ana ve alt kategoriler, ilgili uygulamanın risk seviyesi bilgileri yönetim ekranında görüntülenebilecektir.

**2.6.10.70** Kuruma özel uygulamaların sisteme tanıtılması özel imza oluşturmak suretiyle mümkün olmalıdır.

**2.6.10.71** Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir, sistem yöneticileri tarafında istenirse manuel olarak da güncellenebilir olmalıdır.

**2.6.10.72** İstenmeyen uygulamaları kullandığı tespit edilen ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

**2.6.10.73** Uygulama kontrol veritabanında yer alan tüm uygulamaların listesi, hangi kategoride yer aldıkları ve risk seviyesi bilgisine üreticinin resmi web sitesi üzerinden erişilebilmeli bu bilgiler herkese açık şekilde yayınlanmış olmalıdır.

**2.6.10.74** Sistem yöneticileri tarafından özel uygulama imzaları tanımlamaya izin vermelidir.

**2.6.10.75** Default portlar üzerinden yapılmayan uygulamaların bloklanması sağlanabilmelidir (örneğin 53 portu dışında başka portlardan yapılan DNS trafiği gibi).

**2.6.10.76** Cihaz üzerinde 'rota arama' (route searching) özelliği olması tercih sebebidir. Bu sayede spesifik bir adres için trafiğin hangi rota (route) üzerinden gideceği web arayüzü üzerinden kolaylıkla tespit edilebilmelidir.

**2.6.10.77** Sistemin güncel saldırıların engellenmesi amacıyla aşağıda detayları belirtilen atak engelleme (IPS) özelliği olmalıdır.

**2.6.10.78** IPS sistemi aşağıda belirtilen saldırı tiplerini engelleyebilmelidir.

- **2.6.10.78.1** Trafik Anomaly
- **2.6.10.78.2** Protocol Anomaly
- **2.6.10.78.3** Oran (rate) bazlı saldırılar (brute force gibi)
- **2.6.10.78.4** Sızma temelli (evasive) saldırılar

**2.6.10.79** IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak da yapılabilmelidir.

**2.6.10.80** Her bir IPS imzası için aşağıdaki aksiyonlar alınabilmelidir.

- **2.6.10.80.1** İzin ver
- **2.6.10.80.2** İzin ver ve olay kaydı al
- **2.6.10.80.3** Paketi düşür
- **2.6.10.80.4** Saldırıyı yapanı karantinaya al veya işaretle

**2.6.10.81** Tanımlı saldırı tiplerine göre saldırı yapan ip adresleri süreli veya süresiz olarak karantinaya alınabilmeli veya işaretleyebilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

**2.6.10.82** Veritabanında yer alan imzalar aşağıdaki tanımlara göre filtrelenebilmelidir.

- **2.6.10.82.1** CVE koduna göre
- **2.6.10.82.2** Risk seviyesine göre (Kritik, Yüksek Risk, Orta Risk, Düşük Risk gibi)
- **2.6.10.82.3** Hedef işletim sistemine göre (client ve/veya server)

**2.6.10.83** IPS sistemi aşağıda belirtilen detaylı sızma tekniklerine karşı / imza veritabanında olan imzalar kapsamında koruma sağlayabilmelidir.

- **2.6.10.83.1** IP Packet Fragmentation,
- **2.6.10.83.2** TCP Stream Fragmentation
- **2.6.10.83.3** TCP Stream Segmentation,
- **2.6.10.83.4** RPC Fragmentation,
- **2.6.10.83.5** URL Obfuscation,

**2.6.10.84** IPS sistemi Botnet aktivitelerini tespit edebilmeli ve engelleyebilmelidir.

**2.6.10.85** IPS sistemi zararlı URL adreslerine yapılan erişim isteklerini engelleyebilmelidir.

**2.6.10.86** Sistem IPS loglarında saldırının yönünü gösterebilmelidir (client to server veya server to client)

**2.6.10.87** Farklı kullanıcı veya kullanıcı grupları için farklı IPS politikaları oluşturulabilmelidir.

**2.6.10.88** Cihaz üzerindeki IPS imzaları CVE id lerine, kritiklik seviyelerine ve host (client/server) tipine göre aranabilecektir.

**2.6.10.89** IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza için ayrı ayrı ayarlanabilmelidir.

**2.6.10.90** IPS özelliğinde saldırılara karşı kullanılan filtreler, güncelleme dosyasından ya da internet üzerinden güncellenebilmelidir. Ayrıca eğer istenirse, imza güncellemeleri kullanıcı müdahalesi olmadan otomatik olarak da yapılabilmelidir.

**2.6.10.91** Sistem spoof saldırılarını tespit edebilmelidir.

**2.6.10.92** Sistem üzerinde detayları aşağıda iletilen URL Filtreleme özelliği bulunmalıdır.

**2.6.10.93** Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk url adresi, regex ve wildcard formatında tanımlı adreslere erişime izin verebilmeli veya engelleme yapabilmelidir.

**2.6.10.94** Site içeriği taraması yapabilmelidir. Regex veya wildcard formatında belirtilen metni içeren sitelere erişim engellenebilmeli ya da izin verebilmelidir.

**2.6.10.95** USOM gibi harici karaliste kaynakları engellenebilmeli ve otomatik olarak güncellenebilmelidir.

**2.6.10.96** Sadece URI bazında değil, erişilen ip bazında da kontrol yapabilmelidir.

**2.6.10.97** URL bloklama ekranı özelleştirilebilmelidir.

**2.6.10.98** Farklı kullanıcı ve kullanıcı gruplarına farklı URL filtreleme profilleri uygulanabilmelidir.

**2.6.10.99** Riskli kategorideki web sayfalarında kullanıcının AD kullanıcı ve şifresi ile giriş yapması engellenebilmelidir. Bu sayede özellikle kimlik bilgilerini ele geçirme amaçlı phishing saldırıları engellenebilmelidir.

**2.6.10.100** URL filtreleme özelliği Active Directory ile entegre çalışabilecek bu sayede Active Directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında URL filtreleme kuralları tanımlanabilecektir.

**2.6.10.101** URL bloklama ve uyarı portalı değiştirilebilecektir.

**2.6.10.102** Güncel zararlı yazılımların eriştiği C&C (Command and Control) ve Malware Download URL listelerini dinamik olarak güncelleyebilmelidir.

**2.6.10.103** URL filtreleme özelliğinde XFF (X-forwarded-for) özelliği bulunmalıdır.

**2.6.10.104** Gerçek zamanlı analiz yaparak kimlik hırsızlığına karşı phishing sitelerini ve Java script tabanlı atakları engelleyebilecektir.

**2.6.10.105** Cihazın detayları aşağıda belirtilen sanal güvenlik duvarı özelliği olmalıdır:

**2.6.10.106** Cihaz üzerinden birbirinden izole sanal güvenlik duvarları oluşturulabilmelidir.

**2.6.10.107** Cihaz üzerindeki arayüzler veya sanal arayüzler (vlan) sanal güvenlik duvarları arasında paylaştırılabilmelidir.

**2.6.10.108** Her bir sanal güvenlik duvarı için dedike bir sistem yöneticisi atanabilmeli, sistem yöneticilerinin yetkileri olmayan sanal güvenlik duvarlarına erişimleri engellenebilmelidir.

**2.6.10.109** Sanal güvenlik duvarı oluşturulması işlemi web tabanlı veya üreticinin kendi uygulama arayüzü üzerinden kolayca yapılabilmeli ve çalışan mevcut sistemin reboot edilmesine ihtiyaç olmamalıdır.

**2.6.10.110** Her bir sanal güvenlik duvarı üzerinde açılabilecek maksimum oturum (session) sayısı limitlenebilmelidir.

**2.6.10.111** Cihazın detayları aşağıda belirtilen servis dışı bırakma saldırılarını (DoS) engelleme özelliği olmalıdır.

**2.6.10.112** DoS politikaları ile internetten erişilebilir sistemlere (web server, dns server gibi) yönelik trafikler için eşik değer (threshold) bazlı sınırlandırma yapılabilmelidir.

**2.6.10.113** L3 seviyesinde kaynak ve hedef ip bazında açılabilecek toplam oturum sayısı (session) limitlenebilmelidir.

**2.6.10.114** L4 seviyesinde kaynak ve hedef ip bazında açılabilecek oturum sayısı limitlenebilmelidir.

**2.6.10.115** Sistem portscan ve udpscan saldırılarını tespit edip engelleyebilmelidir.

**2.6.10.116** TCP synflood ve UDP flood saldırılarına karşı aynı kaynaktan aynı anda gelebilecek syn istek sayısı limitlenebilmelidir.

**2.6.10.117** Sistem IPv6 adresleri için de yukarıda belirtilen anti-DoS özelliklerini desteklemelidir.

**2.6.10.118** Belirtilen tüm DoS politika konfigürasyonları cihazın web tabanlı veya üreticinin kendi uygulama arayüzü üzerinden ya da CLI üzerinden yapılabilmelidir.

**2.6.10.119** Cihazın detayları aşağıda listelenen "SSL Deep Inspection" özelliği olmalıdır.

**2.6.10.120** Cihazın SSL Inspection özelliği sadece secure HTTP (HTTPS) trafiği için desteklenmemeli, aşağıdaki protokoller için de araya girerek tarama yapabilmelidir.

**2.6.10.120.1** SMTPS

**2.6.10.120.2** POP3S

**2.6.10.120.3** IMAPS

**2.6.10.120.4** FTPS

**2.6.10.121** İstenen web adresleri, kategorileri ve domain'ler için SSL Inspection istisnası uygulanabilmelidir. Wildcard FQDN istisna objeleri desteklenmelidir.

**2.6.10.122** SSL anomaly'lerini ve yazılan istisnai SSL erişimlerini loglayabilmelidir.

**2.6.10.123** Bağlantıyı daha güçlü SSL-cipher algoritmaları kullanımına zorlama özelliği olmalıdır.

**2.6.10.124** Bağlantıyı TLS 1.2 ve 1.3 protokollerine zorlama özelliği olmalıdır.

**2.6.10.125** Güvenilir olmayan CA'ler tarafından imzalanmış sertifika kullanan sitelere erişimler engellenebilmelidir.

**2.6.10.126** Süresi geçmiş (expired) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

**2.6.10.127** Doğrulama süresi geçmiş (validation timeout) ya da doğrulanamayan (validation failed) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

**2.6.10.128** Client hello mesajı içerisinde SNI kontrolü yapabilmelidir.

**2.6.10.129** Sistemin grafik arayüzü veya CLI aracılığıyla aşağıda belirtilen detaylı trafik analiz işlemleri yapılabilecektir. Grafik arayüzünde gerçek zamanlı olarak bu bilgilerin alınabilmesi tercih sebebidir.

**2.6.10.130** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) isteğinde bulunan kullanıcıların listesi,

**2.6.10.131** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yapılan ve en fazla bağlantı (session) isteğinde bulunulan hedef sunucuların listesi,

**2.6.10.132** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) açılan uygulamaların listesi,

**2.6.10.133** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafiğin yapıldığı network arayüzleri (interface'ler),

**2.6.10.134** Geçmiş döneme ait tehditlerin risk puanlarına ve bağlantı (oturum) sayılarına göre listesi,

**2.6.10.135** Yukarıda belirtilen trafik bilgilerinin detay analizi yapılabilmelidir. Örneğin son 24 saatte en fazla oturum açan (session) kullanıcı tespit edildikten sonra bu oturumların detaylarına (hangi uygulamaları kullanarak hangi hedef sunuculara ve web adreslerine doğru bu bağlantıların açıldığı bilgisine) ulaşılabilmelidir.

**2.6.10.136** Cihazın yönetim arayüzü ya da CLI üzerinden sistemle ilgili aşağıdaki detay bilgilere ulaşılabilmelidir.

**2.6.10.136.1** Seri no, Firmware versiyonu ve Uptime bilgisi,

**2.6.10.136.2** Saniyede oluşan log miktarı (eps),

**2.6.10.136.3** Saniyede oluşan bağlantı isteği sayısı (connection per second),

**2.6.10.136.4** Mevcut oturum (session) sayısı,

**2.6.10.136.5** CPU, Memory ve Disk kullanım değeri,

**2.6.10.136.6** Lisans durumu,

**2.6.10.136.7** Sisteme bağlı olan admin'lerin bilgisi,

**2.6.10.137** Teklif edilen 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, Ping6, IPv6 FQDN adresleri desteklenmelidir.

**2.6.10.138** İşletim sistemi ve yazılım güncellemelerini web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

**2.6.10.139** Sistemin detayları aşağıda belirtilen AntiMalware özelliği olacaktır;

**2.6.10.140** Sistem, asgari HTTP(S), POP3, IMAP, FTP ve CIFS/SMB protokolleri aracılığıyla yapılan malware trafiklerini tespit edip engelleyebilmelidir.

**2.6.10.141** Farklı kullanıcı veya kullanıcı grupları için farklı anti-virüs politikaları oluşturulabilmelidir.

**2.6.10.142** Bilinen virüsler için imza temelli bloklama yapabilmelidir.

**2.6.10.143** Anti-virüs imzaları payload tabanlı olmalıdır, hash tabanlı olmamalıdır.

**2.6.10.144** Akan dosya trafiğini tarayabilmelidir.

**2.6.10.145** Sistem, yukarıda belirtilen protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir.

**2.6.10.146** AntiMalware sistemi internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir.

**2.6.10.147** Arşiv dosyalarının detay analizini yapabilmeli, şifreli (encrypted) arşiv dosyaları engellenebilmelidir.

**2.6.10.148** Malware içerdiği tespit edilen kaynak adresler otomatik olarak karantinaya alınabilmelidir.

**2.6.10.149** Üretici Cyber Threat Alliance (CTA) üyesi olmalıdır.

**2.6.10.150** Sistem üzerinde detayları aşağıda belirtilen DNS Security özelliği bulunmalıdır.

**2.6.10.151** Lokal veya internet DNS sunucularına doğru yapılan DNS sorguları kontrol edilerek istenmeyen domain'ler için yapılan sorgulara sistem yöneticileri tarafından belirlenen ip adresinin döndürülmesi veya istenen DNS trafiğinin bloklanması sağlanabilmelidir.

**2.6.10.152** Karaliste ve beyazliste özelliği olmalıdır.

**2.6.10.153** Sistem üzerindeki DNS Security özelliği ile Lokal veya internet DNS sunucularına doğru yapılan DNS sorguları kontrol edilerek DGA, Phishing, Botnet, Malware, Newly Registered, Newly Observed gibi istenmeyen domain'ler için yapılan DNS sorguları, tehdit istihbarat servisindeki Yapay Zeka, Makine Öğrenmesi algoritmaları veya imza veritabanı da kullanılarak engellenebilmelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

**2.6.10.154** Kaynak ip/ağ, kullanıcı/kullanıcı grubu, hedef ip/ağ ve servis bazında bant genişliği politikası yazılabilmelidir.

**2.6.10.155** Spesifik uygulama (örneğin Youtube) ve uygulama kategorisi (öneğin Update) bazında bant genişliği politikası yazılabilmelidir.

**2.6.10.156** Zaman aralığı bazında bant genişliği politikası yazılabilmelidir (örneğin mesai saatleri içerisinde gibi.).

**2.6.10.157** Aynı session içerisinde trafiğin yönüne göre (IN veya OUT yönünde) bant genişliği politikası yazılabilmelidir.

**2.6.10.158** Firewall kuralları bazında bant genişliği politikası yazılabilmelidir. Böylece ilgili kuralla eşleşen trafiklerin limitlenmesi sağlanabilmelidir.

**2.6.10.159** Cihazın proaktif mimaride otomatik aksiyon alabilme özelliği olmalıdır. Bu özellik sayesinde aşağıdaki olaylardan birisi gerçekleştiğinde otomatik olarak eposta gönderimi veya herhangi bir web servisini tetikleme aksiyonlarını otomatik olarak alabilmelidir. Bu özellik için gereken lisanslar ve/veya ürünler teklife eklenmelidir.

- **2.6.10.159.1** Konfigürasyon değişikliği yapıldığında,
- **2.6.10.159.2** Cihaz kapanıp açıldığında,
- **2.6.10.159.3** Lisans süresi bittiğinde,
- **2.6.10.159.4** Yedekli (cluster) cihazlar arasında geçiş yaşandığında,
- **2.6.10.159.5** AV veya IPS database'i güncellendiğinde,

**2.6.10.160** Sistemde önceden tanımlı herhangi bir olay gerçekleştiğinde (örneğin güncelleme işlemi başarısız olduğunda, AD entegrasyonunda sorun olduğunda, IPSec bağlantısı koptuğunda v.b.)

**2.6.10.161** Önerilecek güvenlik duvarı üreticisi, güncel "Gartner Magic Quadrant Enterprise Network Firewalls" raporunda "Leaders" kategorisinde yer almalıdır veya yerli ürün olmalıdır.

**2.6.10.162** Teklif edilecek tüm ürünler üreticinin global destek merkezi ya da üreticinin yetkilendirdiği distribütör tarafından 7x24 destek hizmeti dahil şekilde tekliflendirilecektir. Kurum, üreticinin global deste merkezine 7x24 case açabilecektir.

**2.6.10.163** Güvenlik Duvarı sisteminin 5 yıl süre ile yazılım/işletim sistemi güncellemelerini ve 5 yıl süre için Güvenlik Duvarı (Firewall), IPSec VPN, SSL VPN, Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Kontrol (Application Control), Virüs/Zararlı İçerik Kontrolü (AV), URL (Web) Filtreleme, DNS Güvenlik Sistemi, SSL-TLS Tarama (Inspection), Bulutta Sıfırıncı Gün Tarama (Cloud Sandbox) lisanslarının özelliklerin tümünün kullanımı için gereken bütün lisanslar teklife eklenmelidir.

**2.6.10.164** Teklif edilecek donanım ve lisanslar Demo, Lab, Spare tipinde olmamalıdır.

**2.6.10.165** Cihaz üzerindeki tüm güç kaynağı yuvaları tamamen dolu olarak teklif edilecektir.

**2.6.10.166** Güvenlik duvarı yönetimi Windows ile erişilmesi gerekmektedir. Macos, linux işletim sistemleri ile erişilebilmesi tercih sebebidir.

**2.6.10.167** Cihazlar, web tabanlı veya üreticinin kendi uygulama arayüzü üzerinden yönetilebilecektir. Web veya uygulama tabanlı yönetim arayüzünden firewall güvenlik politikaları, url filtering, application control, ips, antivirüs, dns güvenliği gibi yapılandırmalar gerçekleştirilebilmelidir. Web tabanlı arayüz ile erişimin olmadığı durumlarda yönetim cihazının yedekli ve tüm lisansları ile teklif edilmesi gerekmektedir.

**2.6.10.168** Firewall üretici ya da üreticinin yetkilendirdiği distribütör desteği minimum aşağıdaki gibi olmalıdır.

I. Telefonla Destek (24/7)
II. Ürün değişim süresi (RMA) (Maksimum 3 iş günü)
III. En Üst Seviyede Mühendis Yardımı (Eskalasyon)
IV. Yerinde destek (Kritik konularda)
V. İleri seviyede sorun analiz ve giderme

### 2.6.11 Güvenlik Duvarı – Pasif DC

**2.6.11.1** Güvenlik duvarı yedekli HA çifti şeklinde teklif edilecektir. Buna göre aynı veri merkezinde aktif cihazda bir sorun olması durumunda; tüm trafik otomatik olarak aynı veri merkezinde konumlanmış pasif cihaza aktarılacaktır. Bu durumda uygulama tanıma ve routing özellikleri pasif cihaz üzerinden bir kesinti olmadan çalışacaktır.

**2.6.11.2** Cihaz, mimari açıdan stateful inspection, IP Paket Filtreleme ve Uygulama Tanıma özelliklerini bünyesinde bulundurmalı ve aşağıdaki güvenlik servislerine sahip olmalıdır. Anti-Virus, DNS Security, URL Filtreleme ve Sıfırıncı Gün Koruma tarafında gelişmiş özelliklerin tümünün kullanılabilmesi için gerekli tüm lisanslar teklife eklenmelidir.

I. Firewall
II. IPSEC VPN, SSL VPN
III. Uygulama kontrolü (Application Control)
IV. Atak Engelleme (IPS)
V. Anti-Virus
VI. Anti-Spyware/Anti-Bot
VII. URL Filtreleme
VIII. DNS Security
IX. Kullanıcı kimliği entegrasyon
X. SSL Inspection
XI. Sıfırıncı gün koruma (Anlık hash sorgusu + on-prem/cloud sandbox desteği)

**2.6.11.3** Teklif edilecek olan her iki sistem port ve performans anlamında birbiriyle aynı marka model ve kapasitede olmalıdır.

**2.6.11.4** Uzun süreli kullanım açısından (End-of-Order, End-of-Sale) teklif edilecek güvenlik duvarı donanım modelinin piyasaya ilk çıkış tarihi belirtilmelidir. Daha yeni olan modeller tercih sebebi olacaktır.

**2.6.11.5** Ürün, yüksek performans ve düşük gecikme ihtiyacı nedeniyle ASIC veya FPGA veya integrated crypto assistant veya İntel tabanlı işlemci mimarisine sahip olması tercih sebebidir. Bu sayede özellikle SSL Deep Inspection gibi yüksek performans gereksinimi duyulan durumlarda performans sorunu yaşanmamalıdır.

**2.6.11.6** Ürün, aşağıda detayları belirtilen OSI mimarisine uygun çok katmanlı güvenlik modeline sahip olmalıdır.

**2.6.11.6.1** Güvenlik politikaları özelinde OSI L4 ve L7 katmanları arasında çalışabilmelidir. Bu sayede istenen trafikler L4 (kaynak ip/kullanıcı, hedef ip, hedef port) istenen trafikler L7 uygulama seviyesinde analiz edilebilmelidir.

**2.6.11.6.2** 7. katmanda uygulama seviyesinde analiz edilmesi gerekmeyen trafikler tipleri için (yedekleme trafiği, database senkronizasyonu v.b.) sistemin gereksiz yere performans tüketmesi engellenebilmeli ve sistem verimliliği arttırılabilmelidir.

**2.6.11.7** Politika özelinde L7 güvenlik servisleri aktif edilebilmelidir. Bu kapsamda aşağıda listelenen güvenlik servisleri tercihe bağlı olarak seçilebilmelidir.

I. Uygulama Kontrolü
II. Atak Engelleme (IPS)
III. AntiVirus, AntiMalware, Anti-Spyware/Anti-Bot
IV. URL/Web Filtreleme
V. DNS Security
VI. Dosya Filtreleme
VII. SSL Inspection

**2.6.11.8** Teklif edilen güvenlik duvarının firewall throughput değeri 35 (otuzbeş) Gbps performansını desteklemelidir. Üreticinin herkese açık dökümanlarında bu değer açıkça belirtilmiş olmalıdır.

**2.6.11.9** Ürün, en az 9 (dokuz) Gbps tehdit engelleme (Firewall, Uygulama Kontrol, IPS, AntiMalware servisleri aktif) performans (throughput) değerine sahip olmalıdır. Üreticinin resmi web sayfasında ilgili değerin herkese açık bir şekilde yayınlanmış olması gerekmektedir.

**2.6.11.10** Ürün en az 14 (ondört) Gpbs IPSEC VPN performans değerine sahip olmalıdır.

**2.6.11.11** Ürün, aynı anda en az 3 (üç) milyon oturumu desteklemelidir.

**2.6.11.12** Ürün, saniyede en az 260.000 (ikiyüzaltmışbin) yeni oturum açabilme kapasitesine sahip olmalıdır.

**2.6.11.13** Ürün, aynı anda en az 8 adet 10GE SFP+ fiber veya 4 adet 25GE SFP28, en az 8 adet 1 GE SFP ve en az 8 adet RJ45 bakır bağlantı desteğine sahip olmalıdır. 10 GE port adetinin sayıca fazla olması ve 10 GE portların 25GE olarak kullanılabilir olması tercih sebebidir. Port "interface" sayıları dinamik "değiştirilebilir" olan üreticiler tüm ethernet kartlarının dolu olacağı max konfigürasyonu önermelidir.

**2.6.11.14** Cihazlar üzerinde en az ikişer adet 1Gbps bakır, sekizer adet 25GBps SFP28 orijinal transceiver ve bağlantı kablosu ile çalışır durumda olmalıdır.

**2.6.11.15** Şartnamede istenen performans ve port değerleri tek bir donanım ile karşılanamaması durumunda üretici firma birebir aynı özelliklere sahip donanım veya şase ürününden birden fazla teklif ederek isterleri kümeleme (clustering) ile sağlayabilecektir. Bu durumda cihazların isterlere uygun çalışabilmesi için gerekli cihaz ve yazılımlar da teklife dahil edilecektir. Kümeleme (clustering) yapılacak cihazların hepsi port ve performans anlamında birbiriyle aynı marka model ve kapasitede olmalıdır.

**2.6.11.16** Kurum kaynaklarına uzaktan güvenli erişiminin sağlanabilmesi için cihaz üzerinde aşağıda detayları belirtilen SSL-VPN özelliği olmalıdır.

**2.6.11.16.1** Cihaz aynı anda en az 1.500 (bin beş yüz) kullanıcının SSL VPN ile bağlantısına izin verebilecek kapasitede olmalıdır.

**2.6.11.16.2** SSL VPN istemcisi en az Windows, Mac OS, Linux, IOS ve Android işletim sistemlerini desteklemelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

**2.6.11.16.3** Farklı kullanıcılara farklı ip adresleri atanmasını desteklemelidir.

**2.6.11.16.4** SSL VPN üzerinden erişen kullanıcıların lokal kullanıcı veritabanı, RADIUS, LDAP veya Microsoft AD üzerinden kimlikleri doğrulanabilmelidir.

**2.6.11.16.5** SSL VPN tüneli içerisinden gelen trafiklerde IPS, Uygulama Kontrolü, AntiMalware, URL Filtreleme özellikleri uygulanabilir olmalıdır.

**2.6.11.16.6** SSL-VPN ile bağlantı yapacak adresler belirtilebilmeli, belirtilen adresler dışından SSL-VPN erişimleri engellenebilmelidir.

**2.6.11.16.7** Split tunnelling özelliği ile sadece belirtilen hedef adresler için trafiğin tünele yönlendirilmesi sağlanabilmelidir.

**2.6.11.16.8** DNS servisi için ayrıca split tunneling'i desteklemelidir. Bu sayede sadece spesifik domain sorguları için merkezdeki DNS sunucularının kullanımı sağlanabilmelidir.

**2.6.11.16.9** SSL-VPN ile bağlanacak kullanıcılar için two factor authentication (2FA) özelliği desteklenmelidir.

**2.6.11.16.10** SSL-VPN ile yapılan aktif bağlantılar monitör edilmelidir. Bağlı olan kullanıcı ve ne zaman login olduğu bilgilerine web tabanlı veya üreticinin kendi uygulama arayüzü üzerinden erişilebilmelidir.

**2.6.11.16.11** SSL-VPN portal özelliği ile son kullanıcı bilgisayarlarına yazılım (vpn agent) kurmadan portal üzerinden SSL VPN yapılabilmelidir. Portal üzerinden HTTP(S), FTP, VNC, RDP ve SSH uygulama ve protokol erişimleri desteklenmelidir.

**2.6.11.17** Firewall üzerinde en az 10 (on) adet sanal firewall oluşturulabilecek lisans ile teklif edilecektir.

**2.6.11.18** Her bir veri merkezi için güvenlik duvarı sistemi yedekli mimaride ikişer adet teklif edilecektir.

**2.6.11.19** Ürün, aktif-aktif ve aktif-pasif yedeklilik senaryolarını desteklemelidir.

**2.6.11.20** Kümeleme yapılan donanımlarda oturumlar donanımın herhangi birisinin arızalanması durumunda oturum kaybı olmadan otomatik olarak diğer güvenlik duvarı cihazı üzerinde devam edebilmelidir.

**2.6.11.21** Network arayüzlerinin herbiri LAN, WAN, DMZ veya kullanıcı tanımlı bir segment olarak konfigüre edilebilmelidir. İlgili arayüzler 802.1q protokolünü desteklemelidir. Her bir interface için Alias tanımı girilebilmelidir.

**2.6.11.22** Saat, gün bazında erişim kontrolü yapabilmelidir.

**2.6.11.23** Yerel ağdaki bir ya da birden fazla adres aralığındaki birçok IP'yi istenirse tek bir adres arkasında, istenirse her bir aralığı başka bir tek adres arkasında saklayabilmeli ya da bire bir adres çevrim özelliği (NAT) olmalıdır.

**2.6.11.24** NAT kuralları, Güvenlik kurallarından bağımsız ayrı kural seti olarak tanımlanabilecektir.

**2.6.11.25** DHCP server ve IPv4/v6 DHCP Relay olarak yapılandırabilecektir.

**2.6.11.26** Tek VLAN üzerinde en az 1000 adet, sanal firewall kullanıldığında ise toplamda en az 4000 adet VLAN desteği sağlamalıdır.

**2.6.11.27** Güvenlik Duvarı 802.3 ad LACP desteklemelidir.

**2.6.11.28** Güvenlik Duvarı SNMP v3 desteklemelidir.

**2.6.11.29** Güvenlik Duvarının Netflow desteği olmalıdır.

**2.6.11.30** Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dâhil edilmelidir.

**2.6.11.31** Yönetim arayüzü veya CLI üzerinden her bir fiziksel, interface için trafik kullanım değerleri gerçek zamanlı ve geçmişe dönük görüntülenebilmelidir. Bu sayede hangi interface üzerinde o an için ne kadar trafik kullanımı olduğu bilgisi (throughput) IN ve OUT yönlü analiz edilebilmelidir.

**2.6.11.32** Sistemin SPI (Stateful Packet Inspection) özelliği olmalıdır.

**2.6.11.33** RIP, OSPF, BGP, static ve kaynak tabanlı (policy based) yönlendirme özelliklerine sahip olmalıdır. Multicast routing'i desteklemelidir.

**2.6.11.34** Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dâhil edilmelidir.

**2.6.11.35** Path monitoring vb özelliği cihaz üzerinde tanımlanan statik route tanımları bağdaştırılabilecektir. Böylece tanımlanan statik yönlendirmeler üzerinden sağlanan erişimlerin çalışıp çalışmadığını kontrol edebilecektir. Erişim olmadığı durumlarda statik yönlendirme satırını yönlendirme tablosundan otomatik olarak kaldırarak alternatif yoldan erişim imkânı sağlanacaktır.

**2.6.11.36** Cihazın Multicast yönlendirme desteği olmalı ve PIM-SM, PIM-SSM, IGMP v1, v2, v3 desteklemelidir.

**2.6.11.37** Site to site ve client to site IPSEC VPN desteği olmalıdır.

**2.6.11.38** Cihaz, IPSec VPN standardını desteklemelidir. IKE şifreleme şemalarını desteklemelidir. 3DES, AES algoritmaları ile paket şifreleme yapabilmelidir. Veri bütünlüğü için MD5 ve SHA1 algoritmalarını desteklemelidir. Diffie-Hellman groups 1, 2 ve 5 (Perfect forward secrecy) desteği olmalıdır.

**2.6.11.39** Cihaz GRE tunnel destekleyecektir.

**2.6.11.40** Cihaz IPv6 IPsec destekleyecektir.

**2.6.11.41** DHCP Server ve DHCP Relay özelliği bulunmalıdır.

**2.6.11.42** NAT64 ve Jumbo frame desteği olmalıdır.

**2.6.11.43** Cihaz üzerindeki portlar Layer3 (routing mod) ve Layer2 (bridge mod) ve Monitoring (TAP mod) katmanlarında çalışabilecektir.

**2.6.11.44** Cihazın yeniden başlatılmasına gerek kalmadan üzerindeki portların çalışma seviyesi (L2, L3, monitoring) istendiği gibi değiştirilebilmelidir.

**2.6.11.45** Ağ arayüzü veya zone bazlı kural yazılmasını desteklemelidir.

**2.6.11.46** Saat, gün, tarih bazında erişim kontrolü yapabilmelidir.

**2.6.11.47** MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılabilecektir. Kullanıcıya göre kural yazma sadece kimlik bilgisi gönderen uygulamalarla sınırlı olmayacaktır. Tutulan kayıtlarda kullanıcı ismi de yer alacaktır.

**2.6.11.48** Kullanıcı entegrasyonu için yönetici (administrator) hesabına ve Active Directory yapısında herhangi bir değişikliğe ihtiyaç olmayacaktır.

**2.6.11.49** Cihaz kendisine kullanıcı doğrulaması yapan sistemlerin gönderdiği syslog veya benzeri mesajları çözerek User-IP mapping işlemini gerçekleştirebilecektir.

**2.6.11.50** Cihaz aynı anda farklı yöntemleri kullanarak farklı kaynaklardan IP-Kullanıcı eşleşmesini sağlayabilecektir.

**2.6.11.51** Kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS, LDAP ve AD üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

**2.6.11.52** Kullanıcı/kullanıcı grubu, kaynak ip/ağ, hedef ip/ağ ve uygulama bazlı bantgenişliği yönetim (QoS) desteği olmalıdır. Grup bazlı ya da uç nokta bazlı QoS yapılabilmelidir. QoS trafik için upload veya download yönünde ve zamana bağlı olarak hat kapasitesinin yüzdesel oranında veya bant genişliği kapasitesine göre tanımlanabilmelidir. Ses/video gibi kritik uygulamalara öncelik (priority) ve garanti bantgenişliği yazılabilmelidir. Belirlenen trafik için maksimum bantgenişliği tanımlama imkanı olmalıdır.

**2.6.11.53** SSL inspection (https trafiğinin açılması) desteği olmalıdır. Bu sayede ssl trafiklerini açarak, uygulama detaylarına göre; QoS, uygulama kuralları yazılabilmelidir.

**2.6.11.54** Sistem üzerinde detayları aşağıda belirtilen uygulama kontrol özelliği bulunmalıdır.

**2.6.11.55** Sistemin uygulama kütüphanesinde en az 2500 (iki bin beş yüz) adet uygulama yer almalıdır.

**2.6.11.56** Uygulama kütüphanesinde yer alan tüm uygulamalar aşağıda belirtilen parametrelere göre kategorize edilmiş olmalıdır.

**2.6.11.56.1** Uygulama davranışına göre (botnet, tünelleme amaçlı, bulut uygulaması, bandwith tüketim odaklı v.b.)

**2.6.11.56.2** Risk seviyesine göre (Critical, High, Medium, Low v.b.)

**2.6.11.56.3** Erişim yöntemine göre (Client-server, browser tabanlı, P2P gibi)

**2.6.11.57** Uygulama kontrol özelliği active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında uygulama kontrol kuralları tanımlanabilecektir.

**2.6.11.58** Veri tabanında yer alan uygulamaların listesi, ilgili uygulamanın yer aldığı ana ve alt kategoriler, ilgili uygulamanın risk seviyesi bilgileri yönetim ekranında görüntülenebilecektir.

**2.6.11.59** Kuruma özel uygulamaların sisteme tanıtılması özel imza oluşturmak suretiyle mümkün olmalıdır.

**2.6.11.60** Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir, sistem yöneticileri tarafında istenirse manuel olarak da güncellenebilir olmalıdır.

**2.6.11.61** İstenmeyen uygulamaları kullandığı tespit edilen ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

**2.6.11.62** Uygulama kontrol veritabanında yer alan tüm uygulamaların listesi, hangi kategoride yer aldıkları ve risk seviyesi bilgisine üreticinin resmi web sitesi üzerinden erişilebilmeli bu bilgiler herkese açık şekilde yayınlanmış olmalıdır.

**2.6.11.63** Sistem yöneticileri tarafından özel uygulama imzaları tanımlamaya izin vermelidir.

**2.6.11.64** Default portlar üzerinden yapılmayan uygulamaların bloklanması sağlanabilmelidir (örneğin 53 portu dışında başka portlardan yapılan DNS trafiği gibi).

**2.6.11.65** Cihaz üzerinde 'rota arama' (route searching) özelliği olması tercih sebebidir. Bu sayede spesifik bir adres için trafiğin hangi rota (route) üzerinden gideceği web arayüzü üzerinden kolaylıkla tespit edilebilmelidir.

**2.6.11.66** Sistemin güncel saldırıların engellenmesi amacıyla aşağıda detayları belirtilen atak engelleme (IPS) özelliği olmalıdır.

**2.6.11.67** IPS sistemi aşağıda belirtilen saldırı tiplerini engelleyebilmelidir.

I. Trafik Anomaly
II. Protocol Anomaly
III. Oran (rate) bazlı saldırılar (brute force gibi)
IV. Sızma temelli (evasive) saldırılar

**2.6.11.68** IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak da yapılabilmelidir.

**2.6.11.69** Her bir IPS imzası için aşağıdaki aksiyonlar alınabilmelidir.

I. İzin ver
II. İzin ver ve olay kaydı al
III. Paketi düşür
IV. Saldırıyı yapanı karantinaya al veya işaretle

**2.6.11.70** Tanımlı saldırı tiplerine göre saldırı yapan ip adresleri süreli veya süresiz olarak karantinaya alınabilmeli veya işaretleyebilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

**2.6.11.71** Veritabanında yer alan imzalar aşağıdaki tanımlara göre filtrelenebilmelidir.

**2.6.11.71.1** CVE koduna göre

**2.6.11.71.2** Risk seviyesine göre (Kritik, Yüksek Risk, Orta Risk, Düşük Risk gibi)

**2.6.11.71.3** Hedef işletim sistemine göre (client ve/veya server)

**2.6.11.72** IPS sistemi aşağıda belirtilen detaylı sızma tekniklerine karşı / imza veritabanında olan imzalar kapsamında koruma sağlayabilmelidir.

I. IP Packet Fragmentation
II. TCP Stream Fragmentation
III. TCP Stream Segmentation
IV. RPC Fragmentation
V. URL Obfuscation

**2.6.11.73** IPS sistemi Botnet aktivitelerini tespit edebilmeli ve engelleyebilmelidir.

**2.6.11.74** IPS sistemi zararlı URL adreslerine yapılan erişim isteklerini engelleyebilmelidir.

**2.6.11.75** Sistem IPS loglarında saldırının yönünü gösterebilmelidir (client to server veya server to client)

**2.6.11.76** Farklı kullanıcı veya kullanıcı grupları için farklı IPS politikaları oluşturulabilmelidir.

**2.6.11.77** Cihaz üzerindeki IPS imzaları CVE id lerine, kritiklik seviyelerine ve host (client/server) tipine göre aranabilecektir.

**2.6.11.78** IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza için ayrı ayrı ayarlanabilmelidir.

**2.6.11.79** IPS özelliğinde saldırılara karşı kullanılan filtreler, güncelleme dosyasından ya da internet üzerinden güncellenebilmelidir. Ayrıca eğer istenirse, imza güncellemeleri kullanıcı müdahalesi olmadan otomatik olarak da yapılabilmelidir.

**2.6.11.80** Sistem spoof saldırılarını tespit edebilmelidir.

**2.6.11.81** Sistem üzerinde detayları aşağıda iletilen URL Filtreleme özelliği bulunmalıdır.

**2.6.11.82** Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk url adresi, regex ve wildcard formatında tanımlı adreslere erişime izin verebilmeli veya engelleme yapabilmelidir.

**2.6.11.83** Site içeriği taraması yapabilmelidir. Regex veya wildcard formatında belirtilen metni içeren sitelere erişim engellenebilmeli ya da izin verebilmelidir.

**2.6.11.84** USOM gibi harici karaliste kaynakları engellenebilmeli ve otomatik olarak güncellenebilmelidir.

**2.6.11.85** Sadece URI bazında değil, erişilen ip bazında da kontrol yapabilmelidir.

**2.6.11.86** URL bloklama ekranı özelleştirilebilmelidir.

**2.6.11.87** Farklı kullanıcı ve kullanıcı gruplarına farklı URL filtreleme profilleri uygulanabilmelidir.

**2.6.11.88** Riskli kategorideki web sayfalarında kullanıcının AD kullanıcı ve şifresi ile giriş yapması engellenebilmelidir. Bu sayede özellikle kimlik bilgilerini ele geçirme amaçlı phishing saldırıları engellenebilmelidir.

**2.6.11.89** URL filtreleme özelliği Active Directory ile entegre çalışabilecek bu sayede Active Directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında URL filtreleme kuralları tanımlanabilecektir.

**2.6.11.90** URL bloklama ve uyarı portalı değiştirilebilecektir.

**2.6.11.91** Güncel zararlı yazılımların eriştiği C&C (Command and Control) ve Malware Download URL listelerini dinamik olarak güncelleyebilmelidir.

**2.6.11.92** URL filtreleme özelliğinde XFF (X-forwarded-for) özelliği bulunmalıdır.

**2.6.11.93** Gerçek zamanlı analiz yaparak kimlik hırsızlığına karşı phishing sitelerini ve Java script tabanlı atakları engelleyebilecektir.

**2.6.11.94** Cihazın detayları aşağıda belirtilen sanal güvenlik duvarı özelliği olmalıdır:

**2.6.11.95** Cihaz üzerinden birbirinden izole sanal güvenlik duvarları oluşturulabilmelidir.

**2.6.11.96** Cihaz üzerindeki arayüzler veya sanal arayüzler (vlan) sanal güvenlik duvarları arasında paylaştırılabilmelidir.

**2.6.11.97** Her bir sanal güvenlik duvarı için dedike bir sistem yöneticisi atanabilmeli, sistem yöneticilerinin yetkileri olmayan sanal güvenlik duvarlarına erişimleri engellenebilmelidir.

**2.6.11.98** Sanal güvenlik duvarı oluşturulması işlemi web tabanlı veya üreticinin kendi uygulama arayüzü üzerinden kolayca yapılabilmeli ve çalışan mevcut sistemin reboot edilmesine ihtiyaç olmamalıdır.

**2.6.11.99** Her bir sanal güvenlik duvarı üzerinde açılabilecek maksimum oturum (session) sayısı limitlenebilmelidir.

**2.6.11.100** Cihazın detayları aşağıda belirtilen servis dışı bırakma saldırılarını (DoS) engelleme özelliği olmalıdır.

**2.6.11.101** DoS politikaları ile internetten erişilebilir sistemlere (web server, dns server gibi) yönelik trafikler için eşik değer (threshold) bazlı sınırlandırma yapılabilmelidir.

**2.6.11.102** L3 seviyesinde kaynak ve hedef ip bazında açılabilecek toplam oturum sayısı (session) limitlenebilmelidir.

**2.6.11.103** L4 seviyesinde kaynak ve hedef ip bazında açılabilecek oturum sayısı limitlenebilmelidir.

**2.6.11.104** Sistem portscan ve udpscan saldırılarını tespit edip engelleyebilmelidir.

**2.6.11.105** TCP synflood ve UDP flood saldırılarına karşı aynı kaynaktan aynı anda gelebilecek syn istek sayısı limitlenebilmelidir.

**2.6.11.106** Sistem IPv6 adresleri için de yukarıda belirtilen anti-DoS özelliklerini desteklemelidir.

**2.6.11.107** Belirtilen tüm DoS politika konfigürasyonları cihazın web tabanlı veya üreticinin kendi uygulama arayüzü üzerinden ya da CLI üzerinden yapılabilmelidir.

**2.6.11.108** Cihazın detayları aşağıda listelenen "SSL Deep Inspection" özelliği olmalıdır.

**2.6.11.109** Cihazın SSL Inspection özelliği sadece secure HTTP (HTTPS) trafiği için desteklenmemeli, SMTPS, POP3S, IMAPS, FTPS protokolleri için de araya girerek tarama yapabilmelidir.

**2.6.11.110** İstenen web adresleri, kategorileri ve domain'ler için SSL Inspection istisnası uygulanabilmelidir. Wildcard FQDN istisna objeleri desteklenmelidir.

**2.6.11.111** SSL anomaly'lerini ve yazılan istisnai SSL erişimlerini loglayabilmelidir.

**2.6.11.112** Bağlantıyı daha güçlü SSL-cipher algoritmaları kullanımına zorlama özelliği olmalıdır.

**2.6.11.113** Bağlantıyı TLS 1.2 ve 1.3 protokollerine zorlama özelliği olmalıdır.

**2.6.11.114** Güvenilir olmayan CA'ler tarafından imzalanmış sertifika kullanan sitelere erişimler engellenebilmelidir.

**2.6.11.115** Süresi geçmiş (expired) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

**2.6.11.116** Doğrulama süresi geçmiş (validation timeout) ya da doğrulanamayan (validation failed) sertifika kullanan sunucu erişimlerini bloklayabilmelidir.

**2.6.11.117** Client hello mesajı içerisinde SNI kontrolü yapabilmelidir.

**2.6.11.118** Sistemin grafik arayüzü veya CLI aracılığıyla aşağıda belirtilen detaylı trafik analiz işlemleri yapılabilecektir. Grafik arayüzünde gerçek zamanlı olarak bu bilgilerin alınabilmesi tercih sebebidir.

**2.6.11.119** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) isteğinde bulunan kullanıcıların listesi,

**2.6.11.120** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yapılan ve en fazla bağlantı (session) isteğinde bulunulan hedef sunucuların listesi,

**2.6.11.121** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafik yaratan ve en fazla bağlantı (session) açılan uygulamaların listesi,

**2.6.11.122** Gerçek zamanlı (anlık) veya geçmişe dönük en fazla trafiğin yapıldığı network arayüzleri (interface'ler),

**2.6.11.123** Geçmiş döneme ait tehditlerin risk puanlarına ve bağlantı (oturum) sayılarına göre listesi,

**2.6.11.124** Yukarıda belirtilen trafik bilgilerinin detay analizi yapılabilmelidir. Örneğin son 24 saatte en fazla oturum açan (session) kullanıcı tespit edildikten sonra bu oturumların detaylarına (hangi uygulamaları kullanarak hangi hedef sunuculara ve web adreslerine doğru bu bağlantıların açıldığı bilgisine) ulaşılabilmelidir.

**2.6.11.125** Cihazın yönetim arayüzü ya da CLI üzerinden sistemle ilgili aşağıdaki detay bilgilere ulaşılabilmelidir.

I. Seri no, Firmware versiyonu ve Uptime bilgisi
II. Saniyede oluşan log miktarı (eps)
III. Saniyede oluşan bağlantı isteği sayısı (connection per second)
IV. Mevcut oturum (session) sayısı
V. CPU, Memory ve Disk kullanım değeri
VI. Lisans durumu
VII. Sisteme bağlı olan admin'lerin bilgisi

**2.6.11.126** Teklif edilen 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, Ping6, IPv6 FQDN adresleri desteklenmelidir.

**2.6.11.127** İşletim sistemi ve yazılım güncellemelerini web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

**2.6.11.128** Sistemin detayları aşağıda belirtilen AntiMalware özelliği olacaktır;

**2.6.11.129** Sistem asgari HTTP(S), POP3, IMAP, FTP ve CIFS/SMB protokolleri aracılığıyla yapılan malware trafiklerini tespit edip engelleyebilmelidir.

**2.6.11.130** Farklı kullanıcı veya kullanıcı grupları için farklı anti-virüs politikaları oluşturulabilmelidir.

**2.6.11.131** Bilinen virüsler için imza temelli bloklama yapabilmelidir.

**2.6.11.132** Anti-virüs imzaları payload tabanlı olmalıdır, hash tabanlı olmamalıdır.

**2.6.11.133** Akan dosya trafiğini tarayabilmelidir.

**2.6.11.134** Sistem, yukarıda belirtilen protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir.

**2.6.11.135** AntiMalware sistemi internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir.

**2.6.11.136** Arşiv dosyalarının detay analizini yapabilmeli, şifreli (encrypted) arşiv dosyaları engellenebilmelidir.

**2.6.11.137** Malware içerdiği tespit edilen kaynak adresler otomatik olarak karantinaya alınabilmelidir.

**2.6.11.138** Üretici Cyber Threat Alliance (CTA) üyesi olmalıdır.

**2.6.11.139** Sistem üzerinde detayları aşağıda belirtilen DNS Security özelliği bulunmalıdır.

**2.6.11.140** Lokal veya internet DNS sunucularına doğru yapılan DNS sorguları kontrol edilerek istenmeyen domain'ler için yapılan sorgulara sistem yöneticileri tarafından belirlenen ip adresinin döndürülmesi veya istenen DNS trafiğinin bloklanması sağlanabilmelidir.

**2.6.11.141** Karaliste ve beyazliste özelliği olmalıdır.

**2.6.11.142** Sistem üzerindeki DNS Security özelliği ile Lokal veya internet DNS sunucularına doğru yapılan DNS sorguları kontrol edilerek DGA, Phishing, Botnet, Malware, Newly Registered, Newly Observed gibi istenmeyen domain'ler için yapılan DNS sorguları, tehdit istihbarat servisindeki Yapay Zeka, Makine Öğrenmesi algoritmaları veya imza veritabanı da kullanılarak engellenebilmelidir. Bu özellik için ek lisans gerekiyorsa teklife eklenmelidir.

**2.6.11.143** Kaynak ip/ağ, kullanıcı/kullanıcı grubu, hedef ip/ağ ve servis bazında bant genişliği politikası yazılabilmelidir.

**2.6.11.144** Spesifik uygulama (örneğin Youtube) ve uygulama kategorisi (öneğin Update) bazında bant genişliği politikası yazılabilmelidir.

**2.6.11.145** Zaman aralığı bazında bant genişliği politikası yazılabilmelidir (örneğin mesai saatleri içerisinde gibi.).

**2.6.11.146** Aynı session içerisinde trafiğin yönüne göre (IN veya OUT yönünde) bant genişliği politikası yazılabilmelidir.

**2.6.11.147** Firewall kuralları bazında bant genişliği politikası yazılabilmelidir. Böylece ilgili kuralla eşleşen trafiklerin limitlenmesi sağlanabilmelidir.

**2.6.11.148** Cihazın proaktif mimaride otomatik aksiyon alabilme özelliği olmalıdır. Bu özellik sayesinde aşağıdaki olaylardan birisi gerçekleştiğinde otomatik olarak eposta gönderimi veya herhangi bir web servisini tetikleme aksiyonlarını otomatik olarak alabilmelidir. Bu özellik için gereken lisanslar ve/veya ürünler teklife eklenmelidir.

I. Konfigürasyon değişikliği yapıldığında,
II. Cihaz kapanıp açıldığında,
III. Lisans süresi bittiğinde,
IV. Yedekli (cluster) cihazlar arasında geçiş yaşandığında,
V. AV veya IPS database'i güncellendiğinde

**2.6.11.149** Sistemde önceden tanımlı herhangi bir olay gerçekleştiğinde (örneğin güncelleme işlemi başarısız olduğunda, AD entegrasyonunda sorun olduğunda, IPSec bağlantısı koptuğunda v.b.)

**2.6.11.150** Önerilecek güvenlik duvarı üreticisi, güncel "Gartner Magic Quadrant Enterprise Network Firewalls" raporunda "Leaders" kategorisinde yer almalıdır veya yerli ürün olmalıdır.

**2.6.11.151** Teklif edilecek tüm ürünler üreticinin global destek merkezi ya da üreticinin yetkilendirdiği distribütör tarafından 7x24 destek hizmeti dahil şekilde tekliflendirilecektir. Kurum, üreticinin global destek merkezine 7x24 case açabilecektir.

**2.6.11.152** Güvenlik Duvarı sisteminin 5 yıl süre ile yazılım/işletim sistemi güncellemelerini ve 5 yıl süre için Güvenlik Duvarı (Firewall), IPSec VPN, SSL VPN, Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Kontrol (Application Control), Virüs/Zararlı İçerik Kontrolü (AV), URL (Web) Filtreleme, DNS Güvenlik Sistemi, SSL-TLS Tarama (Inspection), Bulutta Sıfırıncı Gün Tarama (Cloud Sandbox) lisanslarının özelliklerin tümünün kullanımı için gereken bütün lisanslar teklife eklenmelidir.

**2.6.11.153** Teklif edilecek donanım ve lisanslar Demo, Lab, Spare tipinde olmamalıdır.

**2.6.11.154** Cihaz üzerindeki tüm güç kaynağı yuvaları tamamen dolu olarak teklif edilecektir.

**2.6.11.155** Güvenlik duvarı yönetimi Windows ile erişilmesi gerekmektedir. Macos, linux işletim sistemleri ile erişilebilmesi tercih sebebidir.

**2.6.11.156** Cihazlar, web tabanlı veya üreticinin kendi uygulama arayüzü üzerinden yönetilebilecektir. Web veya uygulama tabanlı yönetim arayüzünden firewall güvenlik politikaları, url filtering, application control, ips, antivirüs, dns güvenliği gibi yapılandırmalar gerçekleştirilebilmelidir. Web tabanlı arayüz ile erişimin olmadığı durumlarda yönetim cihazının yedekli ve tüm lisansları ile teklif edilmesi gerekmektedir.

**2.6.11.157** Firewall üretici desteği ya da üreticinin yetkilendirdiği distribütör desteği minimum aşağıdaki gibi olmalıdır.

I. Telefonla Destek (24/7)
II. Ürün değişim süresi (RMA) (Maksimum 3 iş günü)
III. En Üst Seviyede Mühendis Yardımı (Eskalasyon)
IV. Yerinde destek (Kritik konularda)
V. İleri seviyede sorun analiz ve giderme

### 2.6.12 Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü

**2.6.12.1** Sistem 150 Adet cihazdan (sunucu, router, switch, firewall, IPS gibi) log alabilmelidir.

**2.6.12.2** Sistem 2000 EPS değerini destekleyecek şekilde lisanslanmalıdır.

**2.6.12.3** Sistem donanım olarak veya VMWARE, Hyper-V, KVM gibi Sanal ortamlar üzerinde çalıştırılabilmelidir.

**2.6.12.4** Sistem SIEM özellikleri kısmında belirtilen tüm özellikleri içeren lisanslar ile tekliflendirilmelidir.

**2.6.12.5** Sistem en az 5 yıllık destek ve aşağıda belirtilen özelliklerin çalışması için gerekli tüm lisansı ile beraber tekliflendirilmelidir.

**2.6.12.6** Sistem sanal platform üzerinde çalışabilecek lisanslamalara sahip yazılımsal çözüm veya donanımsal çözüm olarak teklif edilebilir.

**2.6.12.7** Önerilecek SIEM çözümü ölçeklenebilir olabilmeli ve aşağıdaki seçenekler dahilinde kurulumu yapılabilmelidir:

I. Gerektiğinde harici toplayıcılar (collector) ile log toplamak mümkün olabilmelidir.
II. Harici toplayıcılar (collector) topladığı logları korelasyon bileşenine HTTPS protokolü üzerinden gönderebilmelidir.
III. Harici toplayıcılar (collector) logları merkezi birime gönderemediği durumda ise logları kendi üzerinde tutabilmelidir.
IV. Harici toplayıcılar (collector) topladığı logları gönderim öncesinde sıkıştırabilmelidir.
V. Harici toplayıcıların (collector) arızalanması durumunda yeni harici toplayıcılar (collector) sisteme kolaylıkla eklenebilmeli ve kendi üzerinde bir IP yapılandırması dışında bir ayar ve konfigürasyona gerek duymadan hızlıca devreye girebilmelidir.
VI. Harici toplayıcılar (collector) Netflow bilgisi alabilmelidir.
VII. Harici toplayıcılara (collector) gelen kayıtlara (EPS) ve ip adresi sınırı konulabilmelidir.

**2.6.12.8** Keşfedilen sistemlere ip/subnet seviyesinde yer(lokasyon) bilgisi girilebilmelidir. Bu bilgiler CSV dosyası olarak da import edilebilmelidir.

**2.6.12.9** Keşfedilen sistemlerde önemli interface, process ve port'lar seçilerek sadece kritik interface, process ve portlara ilişkin oluşacak yoğunluklar olay (incident) verisi oluşturabilmelidir.

**2.6.12.10** Keşfedilen sistemlerde istenilen disk'lerin doluluk durumu olay (incident) verisi oluşturmada hariç tutulabilmelidir.

**2.6.12.11** Gerçek zamanlı, memory üzerinde korelasyon yapabilmelidir.

**2.6.12.12** Event bilgisi sıkıştırılmış bir halde tutulmalıdır.

**2.6.12.13** İlişkisel bir veri tabanı (Oracle, MSSql gibi) üzerinde event kaydı tutmamalıdır, ilişkisel veri tabanı sadece konfigürasyon veya vaka (incident) kayıtlarının depolanması amacıyla kullanılmalıdır.

**2.6.12.14** Veri toplamak veya cihazlarla haberleşebilmek amacıyla asgari SNMP, WMI, VM SDK, OPSEC, JDBC, Telnet, SSH, JMX protokollerini desteklemelidir.

**2.6.12.15** Log kaynağı olarak eklenen cihazların SNMP/WMI protokolü ile CPU, Memory, session sayısı, disk kullanımları, ağ arayüz bilgileri gibi performans verileri ve sistem üzerinde çalışan uygulama durumu her bir sistem için tanımlanabilen aralıklarda monitör edilebilmelidir.

**2.6.12.16** SIEM sistemi kendine kayıt gönderen sistemlerin dahil olduğu gruplanmış bir envanter sistemine sahip olmalıdır (CMDB)

**2.6.12.17** SIEM sistemi belirli sistemler, kullanıcılar için watch list (gözlem listesi) oluşturarak belirli bir sürede oluşabilecek önceden belirli herhangi bir durumda alarm üretebilmelidir. (Örnek: Bir kullanıcının hesabının kilitlenmesi veya önemli bir process'in down olması)

**2.6.12.18** CMDB sistemi üzerinden XML formatında raporlar export edilebilmelidir.

**2.6.12.19** SIEM sistemi güncel malware ip, malware URL, malware process bilgilerini düzenli aralıklarla merkezi sistemden güncelleyebilmelidir.

**2.6.12.20** SIEM sistemi malware hash bilgilerini merkezi sistem üzerinden veya TAXII protokolü üzerinden harici sistemlerden güncelleyebilmelidir. Ayrıca belli hash bilgilerini de whitelist olarak sınıflandırabilmelidir.

**2.6.12.21** SIEM sistemi User Agent blacklist bilgilerini merkezi sistemden düzenli olarak yenileyebilmelidir ve belli User Agent'leri whitelist olarak kaydedebilmeldir.

**2.6.12.22** SIEM sistemi custom bloklu IP ve domain'leri CVS formatında import edebilmelidir.

**2.6.12.23** SIEM sistemi istenilen network, sistem, storage, servis vb. elemanlarının dahil olduğu birçok servis grubu oluşturabilmelidir.

**2.6.12.24** Önerilen SIEM sistemi yeni cihaz ve log parser (log ayrıştırıcı) tanımlarını merkezi sistem üzerinden alarak sisteme dahil edebilmelidir.

**2.6.12.25** Önerilen SIEM sisteminde olmayan cihazlar için log ayrıştırıcı (log parser) yöntemi bilinen bir yazım sistemi (örneğin XML) ile yazılarak sisteme dahil edilebilmelidir.

**2.6.12.26** Önerilen SIEM sistemi el ile script aracılığı ile dahil edilen sistemler üzerinden belli komut çıktılarını da log ayrıştırıcı (log parser) gibi sistem log kayıtlarına dahile ederek belli durumlarda monitör edilebilmelidir.

**2.6.12.27** Önerilen SIEM sistemi belli log kayıtlarını giriş esnasında hariç tutularak istenirse sadece kaydedilerek herhangi bir işleme tabi tutulmamalı veya giriş esnasında direk silinebilmeli. Bu silinen log kayıtları lisans EPS'den hariç tutulabilmelidir.

**2.6.12.28** SIEM sistemi belirli cihazlardan gelen log kayıtlarını başka cihazlara yönlendirebilmelidir. (Örnek: netflow veya snmp traps)

**2.6.12.29** SIEM sistemi bir syslog paketindeki çok satırlı syslog kayıtlarını ayrıştırabilmelidir.

**2.6.12.30** Alınan log içerisindeki bilgilerin zenginleştirilmesini desteklemelidir. Örneğin hedef adresin hangi ülke ve şehirde bulunduğu bilgisini log kaydının gösterimi sırasında gösterebilmeli ve bu bilgiyi kullanarak analiz yapılabilmesini mümkün hale getirebilmelidir.

**2.6.12.31** Asgari PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls gibi uyumluluk süreçleri için hazır raporlar oluşturabilmelidir.

**2.6.12.32** Takip amaçlı dashboard ekranlarına sahip olmalı slideshow görünümünde olabilmelidir

**2.6.12.33** Dashboard görüntülemesi sırasında asgari Bar, Pie, Line, Table, Combination (line ve table view), Treemap, Scatter graph, Single values, Gauges ve Geographical Map tiplerde verinin görüntülenmesi desteklenmelidir.

**2.6.12.34** Vaka oluşması durumunda script çalıştırma özelliği bulunmalıdır.

**2.6.12.35** API bazlı entegrasyon ile CMDB ve olay bilgileri harci ticketing sistemleri ile entegre olabilmelidir. (serviceNow, ConnectWise vb.)

**2.6.12.36** Dahili ticketing sistemi barındırmalıdır.

**2.6.12.37** Anahtar kelime bazlı arama tüm log alanlarında veya istenilen bir alan dahilinde yapılabilmelidir.

**2.6.12.38** Geçmişe yönelik arama yapılabilmesi desteklenmelidir.

**2.6.12.39** Arama yapılırken boolean filtreler, gruplamalar, zaman bazlı filtreler, regex kullanımı desteklenmelidir.

**2.6.12.40** İstatiksel profiller desteklenmelidir. Örneğin sistem network kullanımında olağan dışı bir artış olduğunu bu sayede anlayabilmeli ve alarm üretebilmelidir.

**2.6.12.41** Zamanlanmış raporların oluşturulması desteklenmelidir. Bu raporlar CSV veya PDF formatında export edilip mail ile gönderilebilmelidir.

**2.6.12.42** SIEM ürünü Web üzerinden GUI/https üzerinden yönetilebilmelidir.

**2.6.12.43** Çözüm cihazlardan toplanan envanter, performans verisi, güvenlik ile log verisinin aynı ekrandan analiz edilmesini sağlayabilmelidir.

**2.6.12.44** Multi-teanent (çok organizasyonlu) desteği olmalıdır. Bu sayede birbirinden bağımsız organizasyon konfigürasyonları ve bunlara erişen kullanıcı yetkilendirmeleri yapılabilmelidir.

**2.6.12.45** Multi-teanent (çok organizasyonlu) yapılanmada belirli sistemler ip seviyesinde ilgili organizasyona atanabilmelidir.

**2.6.12.46** Multi-teanent (çok organizasyonlu) yapılanmada

**2.6.12.47** Rol temelli yönetim desteği olmalıdır, yönetici, standart kullanıcı, sadece görüntüleme özelliklerinin yanı sıra aşağıdaki şekilde roller oluşturulabilmelidir.

**2.6.12.47.1** Sadece Network sistemlerinin kayıtlarını yönetebilme

**2.6.12.47.2** Sadece Windows sistemlerinin kayıtlarını yönetebilme

**2.6.12.47.3** Sadece Unix sistemlerinin kayıtlarını yönetebilme

**2.6.12.47.4** Sadece Güvenlik sistemlerinin kayıtlarını yönetebilme

**2.6.12.48** Kullanıcı kimlik doğrulaması local veya harici LDAP/Radius sisteminden yapılabilmelidir.

**2.6.12.49** SIEM ürünü zamanı belirlenebilen düzenli rapor bilgileri mail veya scp ile gönderebilmelidir,

**2.6.12.50** SIEM sistemi olay (incident) bilgilerini kendi üzerinde gösterebildiği gibi SNMP Trap (v1, v2c), XML https üzerinden harici sistemlere gönderebilmelidir.

**2.6.12.51** SIEM sistemi olay (incident) bilgilerini otomatik çağrı açabilen sistemlere WSDL üzerinden göndererek acil müdahale edilmesini sağlayabilmelidir.

**2.6.12.52** SIEM sistemi kendine dahil olan tünelleme uygun sistemlere gerektiğinde uzaktan tünel kurarak sisteme müdahale edebilmelidir. (ssh, wmi vb.)

**2.6.12.53** SIEM sistemi raporlarında firma logosunun konulmasına izin vermelidir.

**2.6.12.54** SIEM sistem kaynak kullanımları (memory, CPU, disk vb.) toplam ve process olarak da ayrıntılı şekilde gösterilmelidir. Aşırı artışlarda alarm oluşturulabilmelidir.

**2.6.12.55** SIEM sistemi belli zaman aralıklarında kayıtları arşivleyebilmeli ve arşivlenmiş verileri görüntülenmek üzere geri yükleyebilmelidir.

**2.6.12.56** SIEM sistemi herhangi bir tarihte oluşan herbir event'i bir checksum algoritması (örneğin sha256) üzerinden doğrulayabilmelidir.

### 2.6.13 E-Posta Güvenliği Ürünü

**2.6.13.1** Teklif edilecek e-posta koruma sistemi, kuruma gelen e-postalar üzerinde Spam, zararlı yazılım ve Teklif edilecek e-posta koruma sistemi, kuruma gelen e-postalar üzerinde Spam, zararlı yazılım ve oltalama (phishing) içeriklerini tespit edecek ve engelleyebilecektir.

**2.6.13.2** Sistem sıkılaştırılmış, üreticiye ait işletim sistemi üzerinde çalışmalıdır.

**2.6.13.3** Sistem, şartnamede istenen özellikleri tek bir donanımsal (Donanım / Yazılım Bütünü) çözüm veya sanal yazılımsal çözüm olarak sağlamalıdır.

**2.6.13.4** IPv6 desteği olmalıdır.

**2.6.13.5** Teklif edilen e-posta koruma sistemi, aynı anda E-posta Sunucuya doğru (Inbound) ve E-posta Sunucudan dışarı (Outbound) e-posta trafiğinde güvenlik sağlayabilmelidir.

**2.6.13.6** Erişim Kontrol kuralları ile belirlenen gönderici ve alıcı arasındaki e-posta iletişiminin taranması ve/veya taranmadan iletilebilmesi sağlanabilmelidir.

**2.6.13.7** Alıcı ve gönderici adres tanımlamaları regex ifadesi kullanarak yazılabilmelidir.

**2.6.13.8** IP bazlı politikalar ile kaynak ve hedef IP veya IP grupları arasındaki trafik için uygulanacak smtp protokol ve içerik taraması kontrol edilebilmelidir.

**2.6.13.9** Sistem üzerinden IP bazında bağlantı sınırı, her bir bağlantı üzerinden gönderilebilecek e-posta sayısı ve e-postaların maksimum alıcı adres sayısı belirlenebilmelidir.

**2.6.13.10** Gönderici doğrulaması için SPF kontrolü olmalıdır.

**2.6.13.11** Spam engelleme politikası, e-posta adresi, IP adresi veya domain parametreleri bazında yapılabilmelidir.

**2.6.13.12** Teklif edilen E-posta Güvenlik Sistemi, E-posta Sunucuya doğru (Inbound) e-posta trafiğinde:

**2.6.13.12.1** DOS saldırılarını engelleme (mail bombing),

**2.6.13.12.2** Spam ve Phishing Engelleme,

**2.6.13.12.3** Virus, Spyware ve Malware engelleme,

**2.6.13.12.4** İhtiyaç durumunda, kanuni gerekçelerle E-posta trafiğinin arşivlenmesi fonksiyonlarını sağlamalıdır.

**2.6.13.13** Sistem DOS ataklarına karşı aşağıdaki metotları kullanarak engelleme yapabilmelidir.

**2.6.13.13.1** Belirlenen zaman içerisinde her istemci bazında bağlantı sayısı

**2.6.13.13.2** Her istemci için eş zamanlı bağlantı sayısı

**2.6.13.13.3** Toplam eş zamanlı bağlantı sayısı

**2.6.13.13.4** Her oturum bazında gönderilebilecek e-posta sayısı

**2.6.13.13.5** E-posta içerisinde bulunabilecek alıcı sayısı

**2.6.13.13.6** Alıcı ve gönderen adresleri içeren yasaklı ve izinli e-posta adres listeleri

**2.6.13.14** Teklif edilen E-posta Güvenlik Sistemi, E-posta Sunucudan dışarı doğru (Outbound) e-posta trafiğinde:

**2.6.13.14.1** E-posta sunucudan dışarıya doğru spam engelleme yaparak, kurumun Spam kara listelerine (RBL, DNSBL) girmesini engelleme,

**2.6.13.14.2** Spam ve Phishing Engelleme,

**2.6.13.14.3** Virus, Spyware ve Malware engelleme,

**2.6.13.14.4** Spam Zombie'lerini ve Bot'larını engelleme,

**2.6.13.14.5** İhtiyaç durumunda, kanuni gerekçelerle E-posta trafiğinin arşivlenmesi fonksiyonlarını sağlamalıdır.

**2.6.13.15** E-posta Güvenlik sistemi aşağıdaki metodları kullanarak Spam engelleme yapabilmelidir

**2.6.13.15.1** IP bazında engelleme,

**2.6.13.15.2** İçerik Filtreleme,

**2.6.13.15.3** E-posta Domain ve E-posta adres tabanlı Black/White listelerine göre filtreleme,

**2.6.13.15.4** E-posta Header inceleme

**2.6.13.15.5** RBL ve DNSBL bazlı Filtreleme,

**2.6.13.15.6** E-posta içeriğindeki olabilecek URL ler bazında Filtreleme,

**2.6.13.15.7** Kullanıcı/Domain bazlı filtreleme,

**2.6.13.15.8** Dinamik Heuristic kural güncellemeleri ile filtreleme,

**2.6.13.15.9** Greylist,

**2.6.13.15.10** PDF dosyası içinde içerik tarama,

**2.6.13.15.11** Anahtar kelime bazlı içerik filtreleme

**2.6.13.15.12** İstenmeyen eklenti türlerini filtreleme

**2.6.13.15.13** Bulut istihbarat tabanlı filtreleme.

**2.6.13.16** Taranan maillerde zararlı ya da istenmeyen içerik tespit edildiğinde aşağıdaki aksiyonlar alınabilecektir.

**2.6.13.16.1** İletme

**2.6.13.16.2** Mailin içeriğinde, konusunda, değişiklik yaparak iletme

**2.6.13.16.3** Alıcıya ya da belirlenen alıcılara maili ekte iletme

**2.6.13.16.4** Alıcıya ya da belirlenen alıcılara uyarı ve bilgilendirme gönderme

**2.6.13.16.5** Göndericiye hata mesajı gönderme

**2.6.13.16.6** Göndericiye hata göndermeden maili düşürme

**2.6.13.16.7** Karantinaya alma

**2.6.13.16.8** Mailin konusuna ya da içeriğine istenilen uyarı mesajı ekleme

**2.6.13.17** Sistem, aşağıdaki SMTP fonksyonlarını destekleyecektir

**2.6.13.17.1** RFC5321 SMTP desteği

**2.6.13.17.2** RFC3207 Secure SMTP over TLS desteği

**2.6.13.17.3** RFC4871 DKIM signing and verification desteği

**2.6.13.17.4** RFC4408 Sender Policy Framework verification desteği

**2.6.13.18** E-posta koruma sistemi e-postlara eklenerek gönderilebilecek zararlı yazılımları tespit edebilecek ve engelleyebilecektir. Zararlı yazılım tespit imza veritabanı üretici tarafından internet üzerinden güncellenmelidir.

**2.6.13.19** Reverse DNS kontrolü yapabilmelidir.

**2.6.13.20** Herhangi bir politika sebebi ile engellenmesi gereken e-postalar karantinaya alınabilmeli, istendiği durumda alıcısına karantinadan çıkartılarak iletilebilmelidir.

**2.6.13.21** Karantinaya alınan mailler sistemin kendi üzerinde tutulabileceği gibi, harici bir NFS alanına da yazılabilmelidir.

**2.6.13.22** Spam tespit edilemeyen şüpheli e-postlar için konu bölümüne uyarı eklenebilmelidir.

**2.6.13.23** Kullanıcıların karantinaya düşen e-postları için bilgilendirme e-postaları otomatik olarak gönderilebilmelidir

**2.6.13.24** Kullanıcılar karantinaya düşmüş e-postlarını bir web ara yüzü vasıtası ile karantinadan çıkarabilmelidir.

**2.6.13.25** E-posta ayrı Güvenlik Sistemi, ayrı lisanslamaya gerek kalmadan;

**2.6.13.26** Sistem herhangi bir e-posta sunucu gibi (MTA) çalışabilecek içeri ve dışarı yönde e-posta alıp verirken güvenlik denetimlerini gerçekleştirebilmelidir.

**2.6.13.27** E-posta güvenlik sistemi birden fazla e-posta alan adı ve birden fazla e-posta sunucusu ile çalışabilecektir.

**2.6.13.28** Desteklenen e-posta domain sayısı adedi en az 70 olmalıdır.

**2.6.13.29** E-posta koruma sisteminin depolama kapasitesi en az 2TB olmalıdır.

**2.6.13.30** Sistemin saatte yönlendirebildiği e-posta sayısı en az 65.000 olmalıdır.

**2.6.13.31** AV ve AntiSpam koruması devrede iken saatte tarayabildiği e-posta sayısı en az 50.000 olmalıdır.

**2.6.13.32** Sistem aşağıdaki yöntemler ile yönetilebilmelidir:

**2.6.13.32.1** Web ara yüz üzerinden,

**2.6.13.32.2** Command line üzerinden

**2.6.13.33** Web ara yüzünden yönetim amaçlı güvenli erişim(https) yapılabilmelidir.

**2.6.13.34** Yönetim için ayrı bir sistem gerekmemelidir.

**2.6.13.35** Aynı model ikinci cihazın sisteme eklenmesi durumunda yönetimsel yedeklilikte sağlayabilecek mimaride olmalıdır.

**2.6.13.36** SNMP desteği olmalıdır.

**2.6.13.37** Web ara yüz üzerinden veya TFTP ile yazılım güncellemesi yapılabilmelidir.

**2.6.13.38** E-posta koruma Sistemi kapsamlı kayıt (log) tutabilmeli ve raporlar üretebilmelidir.

**2.6.13.39** Raporlar web ara yüzü üzerinden görülebileceği gibi aynı zamanda belirlenen aralıklarda otomatik oluşturulup e-posta ile gönderimi de sağlanabilmelidir.

**2.6.13.40** Harici Syslog sunucularına kayıt (log) gönderebilecektir.

**2.6.13.41** Teklif, en az 5 (beş) yıl süre ile en az 300 adet e-posta kutusu için yazılım güncelleme, AntiSpam ve AntiVirus/AntiMalware hizmetlerini barındıracak şekilde lisans teklif edilecektir.

**2.6.13.42** Sistem üzerinde dışarı çıkmaması istenen e-posta adresleri otomatik olarak belirlenen başka adresler ile değiştirilebilmelidir.

**2.6.13.43** ÜRÜN, üzerinde, diğer motorlar tarafından tanımlanamayan ancak şüpheli görülen e-posta eklentilerinin izole bir ortamda derinlemesine analiz edileceği kum havuzu (sandbox) olarak adlandırılan sanal bilgisayar sistemi bulunduracaktır.

**2.6.13.44** ÜRÜN, üzerinde, aynı anda çalışan en az 8 (otuz) kum havuzu makinesi desteği olacaktır.

**2.6.13.45** ÜRÜN, üzerinde aynı anda çalışabilen 3 (üç) farklı kum havuzu (sandbox) makinesi desteği olacaktır.

**2.6.13.46** ÜRÜN, bulduğu zararlı e-postlar ile ilgili her türlü bilgiyi (mesaj içeriği, eposta ekran görüntüsü, mesaj başlıkları vb.) tutabilmeli, gerektiğinde detaylı analiz için dosyaların indirilmesine imkan verebilmelidir.

**2.6.13.47** ÜRÜN, kullanıcı tarafından "manual submission" yöntemi ile verilen .eml uzatılı epostaları tarayabilecektir.

### 2.6.14 Web Güvenliği Ürünü

**2.6.14.1** WAF ürünü özel olarak üretici tarafından hedefe yönelik tasarlanmış ve özelleştirilmiş ASIC donanım mimarisi üzerinde çalışmalıdır veya sanal platform üzerinde çalışan sanal yazılım çözümü olarak da teklif edilebilir.

**2.6.14.2** WAF ürünü L3 olarak konumlandırılabilmeli, SSL Offload yapabilmeli ve yükü uygulama sunucularına dağıtabilmelidir.

**2.6.14.3** WAF ürünü SSL trafiğini açıp koruma sağlayabilmelidir.

**2.6.14.4** WAF ürünü offline olarak konumlandırılabilmeli, mirror trafik üzerinden izleme yaparak web trafiğini analiz edebilmeli ve raporlayabilmelidir.

**2.6.14.5** WAF ürünü bir loadbalancer önüne konumlandırıldığında istek paketlerine XFF header'ı ekleyerek orjinal istemci IP'sini arkaya iletebilmelidir.

**2.6.14.6** WAF ürünü loadbalancer ya da reverse proxy görevi gören bir cihaz ile uygulama sunucuları arasına konumlandırıldığı durumda eğer orjinal client IP (X-Forwarded-For) HTTP header'ları ile birlikte gönderiliyorsa bu IP'yi yorumlayabilmeli, bu IP üzerinden üreticinin istihbarat ağına IP Reputasyon sorgusu yapabilmeli ve Saldırı Loglarında görüntüleyebilmelidir.

**2.6.14.7** WAF ürünü IPv6 desteklemelidir.

**2.6.14.8** WAF ürünü kendi içerisinde sanallaştırmaya uygun olmalı böylelikle birden fazla uygulama sahibine ayrı ayrı hizmet edebilmeli, farklı uygulamalara farklı yönetici hesapları ile erişime olanak tanıyabilmeli ve raporlayabilmelidir.

**2.6.14.9** WAF ürünü üzerinde web tarama araçlarının çıktıları sonucunda yeni güvenlik politikaları üretilebilmelidir veya cihaz yöneticisi mevcut kuralları güncelleyebilmelidir.

**2.6.14.10** WAF ürünü coğrafi trafik analizi yapabilmeli ve bunu görsel olarak sunabilmelidir.

**2.6.14.11** WAF ürünü Aktif-Pasif yedekli mimaride çalışmayı desteklemelidir.

**2.6.14.12** WAF ürünü SSH/HTTPS protokollerini kullanarak uzaktan yönetime izin vermelidir.

**2.6.14.13** WAF ürünü Komut Satırı ve Web Arayüzü yönetim konsolları sunmalıdır.

**2.6.14.14** Teklif edilecek WAF ürününün sanal platform desteğinin olması tercih sebebidir.

**2.6.14.15** WAF ürünü uygulamada kullanılan parametreler için öntanım yapmaya veya otomatik öğrenmeye olanak tanıyabilmelidir. Pozitif güvenlik modelini desteklemelidir.

**2.6.14.16** Güvenlik uzmanı koruma ile öğrenme politikalarını ayrı ayrı düzenleyebilmeli, ikisinden biri üzerinde çalışırken diğerini etkilememelidir.

**2.6.14.17** WAF ürünü IP reputasyonuna göre otomatik olarak bilinen botnet, malicious hosts, anonymous proxy'ler ve D/DoS kaynaklarını engelleyebilmeli, kısa periyodlarla saldırı yapan IP adreslerini kontrol ederek güncel tehdit olup olmadığını kontrol etmeli ve duruma göre otomatik olarak karalisteye ekleyip çıkarabilmelidir.

**2.6.14.18** WAF ürünü içerik çalma (Content Scrapping) saldırılarına karşı koruma sağlamalıdır.

**2.6.14.19** WAF ürünü kendi içerisinde antivirüs motoruna sahip olmalıdır veya ICAP protokolü desteği ile antivirüs entegrasyonu yapılabilmelidir.

**2.6.14.20** WAF ürünü dosya upload işlemlerinde dosya boyutuna göre kısıtlama sağlayabilmelidir.

**2.6.14.21** WAF ürünü dosya upload işlemlerinde dosya tipine göre kısıtlama sağlayabilmelidir.

**2.6.14.22** WAF ürünü üzerinde korunacak uygulama bazında herhangi bir lisans limitasyonu bulunmamalıdır.

**2.6.14.23** WAF ürünü TOP 10 OWASP açıklıklarına karşı otomatik koruma sağlamalı, koruma imzaları üretici tarafından rutin olarak güncellenmelidir.

**2.6.14.24** WAF ürününe ait koruma imzaları belli bir mantığa göre gruplanmış ve arama yapılabilir olmalıdır.

**2.6.14.25** WAF ürünü, koruduğu uygulamanın önceden tanımlanmış dizinlerini öğrenip izleyebilmelidir.

**2.6.14.26** WAF ürünü uygulama seviyesindeki D/DoS ataklarını anlayabilmeli ve engelleyebilmelidir.

**2.6.14.27** WAF ürünü uygulama seviyesinde "Src IP tabanlı HTTP Request limitasyonu" ve "Aynı http cookie ile HTTP İsteği" şeklindeki DoS korumalarını sağlayabilmelidir.

**2.6.14.28** WAF ürünü bot ve robot koruması kapsamında bilinen arama motorlarını ayırt edebilmeli ve kötü arama motorlarını ve robotları (scannerlar, crawlerlar, spiders) engelleyebilmelidir.

**2.6.14.29** WAF ürünü URL, HTTP Request Header, HTTP Response Header, URL Parametresi ve HTTP Response kodu için kullanıcının özel imza yazmasına olanak tanımalı ve her biri için farklı aksiyonlar alabilmelidir.

**2.6.14.30** WAF ürünü cookie poisoning, schema poisoning gibi saldırıları anlayabilmeli ve koruma sağlamalıdır.

**2.6.14.31** WAF ürününün SYN Cookie özelliği olmalıdır.

**2.6.14.32** WAF ürünü gizli form alanlarına karşı koruma politikası yazmaya izin vermelidir.

**2.6.14.33** WAF ürünü "XSS", "SQL Injection", "CSRF", "Directory Traversal", "Buffer Overflow", "Remote File Inclusion", "Command Injection" ataklarına karşı koruma sağlamalıdır. "File upload" analizi yapabilmelidir.

**2.6.14.34** WAF ürünü üzerinde bulunan her bir imza gerektiğinde profil bazlı kapatılabilmeli ya da imza bazında IP beyazlistesi uygulanabilmelidir.

**2.6.14.35** WAF ürününün saldırı logundan kısayol ile beyazliste (exclusion) yazılabilmelidir.

**2.6.14.36** WAF ürünü "Klasör Listeleme", "Sunucudan Dönen Hata Yanıtları" gibi bilgi sızıntısına yol açabilecek konfigürasyon hatalarına karşı önlem alabilmelidir.

**2.6.14.37** WAF ürünü URL encoding veya parametre/header encoding yapılmış saldırılara karşı decoding yapabilmeli ve atak paternini tespit edebilmelidir.

**2.6.14.38** WAF ürünü HTTP RFC (7230-7235 veya 7236) 'ye göre uyumluluk kontrolü sağlamalı, RFC uyumluluğu olmayan (malformed) HTTP isteklerini engelleyebilmelidir.

**2.6.14.39** WAF ürünü bilinen ataklara karşı imza veritabanına sahip olmalı, bu veritabanı üretici tarafından rutin olarak güncellenmelidir.

**2.6.14.40** WAF ürününün web trafiğini otomatik öğrenme ve öğrendiği trafiğe göre otomatik olarak koruma politikası oluşturabilme özelliği olmalıdır.

**2.6.14.41** WAF ürünü üzerinde otomatik öğrenilecek alanlara özel tanım yapılabilmeli, böylelikle bu alanlarda öğrenmeye dahil edilebilmelidir.

**2.6.14.42** HTTPS şifrelemesi SSLv3, TLS1.0, TLS1.1 ve TLS1.2 desteklemeli, gerektiğinde istenen şifreleme metodu kapatılabilmelidir.

**2.6.14.43** HTTPS şifreleme için poodle, heartbleed gibi zafiyetlere karşı sıkılaştırılmış politikalar ile koruma sağlanmalıdır.

**2.6.14.44** WAF ürünü aynı zamanda yük dengeleme özelliğine sahip olmalıdır.

**2.6.14.45** WAF ürünü yük dengeleme yaparken aşağıdaki algoritmaları kullanabilmelidir;

- **2.6.14.45.1** Round Robin
- **2.6.14.45.2** Weighted Round Robin
- **2.6.14.45.3** Least Connection

**2.6.14.46** WAF ürünü yük dengeleme özellikleri içerisinde "Persistency" özelliğine sahip olmalıdır. Aşağıdaki persistency kabiliyetlerini sunabilmelidir;

- **2.6.14.46.1** Persistent IP
- **2.6.14.46.2** Persistent Cookie
- **2.6.14.46.3** Insert Cookie

**2.6.14.47** WAF ürünü uygulamanın içerisinde kullanılan giriş alanlarından kullanıcı isimlerini okuyabilmeli ve hem trafik loglarında hem de saldırı loglarında "Username" alanında gösterebilmelidir. Böylelikle kuruma özel kullanıcıların tüm hareketlerinin izlenmesine olanak sağlayacaktır.

**2.6.14.48** WAF ürünü SIEM ürünleri ile Log entegrasyonu sağlayabilmelidir.

**2.6.14.49** WAF ürününün yönetim arayüzünde (GUI) saldırı logları açık bir şekilde görüntülenebilmelidir.

**2.6.14.50** WAF ürününün yönetim arayüzünde (GUI) saldırı logları gruplanmış şekilde görüntülenebilmeli, böylelikle fazla sayıda oluşabilecek saldırı logları sonucunda sistem yöneticisine görsel kolaylık sağlamalıdır.

**2.6.14.51** WAF ürünü yönetim arayüzünde (GUI) web erişim logları görüntülenebilmeli, bunun için ek yazılım ya da donanıma ihtiyaç duyulmadan loglara rahatlıkla erişim sağlanmalıdır.

**2.6.14.52** WAF ürününün kendi arayüzünden trafiğin yönlendirildiği sunucu, kaynak IP, hedef IP, erişilen hostname, url, http istek başlık bilgileri, http cevap başlık bilgileri, istek süresi, cevap süresi, http yanıt kodu (200, 404, 500 vs.) bilgileri mutlaka bulunmalıdır.

**2.6.14.53** WAF ürünü üzerinden müşteriye özel olarak rapor oluşturmaya olanak tanımalıdır, bunun için ek yazılım ya da donanıma ihtiyaç duyulmadan loglara rahatlıkla erişim sağlanmalıdır.

**2.6.14.54** WAF ürünü PDF veya MHT formatlarında rapor çıktısı üretebilmelidir.

**2.6.14.55** WAF ürünü minimum 500 Mbps Advance WAF http/https trafiğini işleyebilme kapasitesine sahip olmalıdır.

**2.6.14.56** WAF ürünü yedekli çalışmayı desteklemelidir.

**2.6.14.57** WAF ürünü donanımsal çözüm olabileceği gibi yazılımsal ve sanal çözüm olabilir. Sanal çözüm teklif edildiği takdirde, üzerinde çalışacağı VM veya sanal platformu ve gerekli CPU, RAM ve depolama alanı gibi teknik ihtiyaçları kurum kendisi sağlayacaktır.

**2.6.14.58** Sistemin IP Reputation fonksiyonlarının 5 yıl süre ile Yazılım/işletim sistemi güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

### 2.6.15 Sunucu Güvenliği Ürünü

**2.6.15.1** Teklif edilecek ürünün ana amacı, kurum bünyesinde bulunan sanal veya fiziksel ortamdaki sunucuların ve aynı zamanda bulut üzerinde çalıştırılması planlanan sanal sunucuların güvenliğinin sağlanmasıdır.

**2.6.15.2** Teklif edilecek ürünün sanal ve fiziksel sunucuların güvenliği için özel olarak geliştirilmiş bir ürün olması talep edilecektir. Standart uç nokta güvenliği çözümleri, sanallaştırma altyapısında kullanıma uygun olmadığı için, bu ürün gamı kapsamında değerlendirilmemektedir.

**2.6.15.3** Teklif edilecek ürün, sanal ortamda sanal makinalara bir ajan kurulumu ile de zararlı yazılım koruması yapabilmelidir.

**2.6.15.4** Teklif edilecek ürün, merkezi bir panelden yönetilebilmelidir.

**2.6.15.5** Ürün, kendi üzerindeki zararlı yazılım ve ağ atakları imza altyapısını sürekli güncelleyebilmelidir.

**2.6.15.6** Ürün hem firmanın kendi sanal ortamları hem de Amazon AWS gibi bulut ortamlarındaki sanal makinaların tek bir panelden yönetilmesini sağlamalıdır.

**2.6.15.7** Ürünün yönetim konsolu, AWS API üzerinden Amazon AWS'deki çalışan sanal makinaların keşfedilmesini veya güvenlik yazılımının yönetimini yapabilmelidir.

**2.6.15.8** Ürün, sanal makinalar için aşağıdaki işletim sistemlerini desteklemelidir:

- **2.6.15.8.1** Windows 11 21H2 Pro/Enterprise/Education
- **2.6.15.8.2** Windows 10 Desktop Pro 19H1/19H2/20H1/20H2/21H1 (32 / 64-bit)
- **2.6.15.8.3** Windows 10 Enterprise 2016 LTSC/2019 LTSC/19H1/19H2/20H1/20H2/21H1 (32 / 64-bit)
- **2.6.15.8.4** Windows 8.1 Update 1 Professional/Enterprise (32 / 64-bit)
- **2.6.15.8.5** Windows 7 Professional/Enterprise Service Pack 1 (32/64-bit)
- **2.6.15.8.6** Windows Server 2022 Standard/Datacenter/Essentials (Desktop experience/Core)
- **2.6.15.8.7** Windows Server 2019 Standard/Datacenter (Desktop experience/Core)
- **2.6.15.8.8** Windows Server 2016 Standard/Datacenter (Desktop experience/Core)
- **2.6.15.8.9** Windows Server 2012 R2 Standard/Datacenter/Essentials (Desktop experience/Core)
- **2.6.15.8.10** Windows Server 2012 Standard/Datacenter/Essentials (Desktop experience/Core)
- **2.6.15.8.11** Windows Server 2008 R2 Service Pack 1 Standard/Enterprise/Datacenter (Desktop experience/Core)
- **2.6.15.8.12** CentOS 8.0 ve üzeri (64-bit)
- **2.6.15.8.13** CentOS 7.3 ve üzeri (64-bit)
- **2.6.15.8.14** Debian GNU/Linux 10.1 ve üzeri (32/64-bit).

**2.6.15.8.15** Debian GNU/Linux 9.4 ve üzeri (32/64-bit)

**2.6.15.8.16** Oracle Linux 8.0 ve üzeri (64-bit)

**2.6.15.8.17** Oracle Linux 7.3 ve üzeri (64-bit)

**2.6.15.8.18** Red Hat Enterprise Linux Server 8.0 ve üzeri (64-bit).

**2.6.15.8.19** Red Hat Enterprise Linux Server 7.3 ve üzeri (64-bit)

**2.6.15.8.20** SUSE Linux Enterprise Server 15 SP2 (64-bit)

**2.6.15.8.21** Ubuntu 20.04 LTS (64-bit).

**2.6.15.8.22** Ubuntu 18.04 LTS (64-bit).

**2.6.15.9** Teklif edilecek ürün sanal makinalarda mevcut olan zararlı yazılımları tespit edebilmelidir.

**2.6.15.10** Teklif edilecek ürün rootkit tarzı zararlı yazılımlara karşı önlem sağlamalıdır.

**2.6.15.11** Teklif edilecek ürün bilinmeyen zararlılara karşı sezgisel analiz yöntemleriyle önleme yapabilmelidir.

**2.6.15.12** Teklif edilecek ürün, üretici firmaya ait bulut-bazlı bir tehdit istihbarat servisi üzerinden yeni tehditlere karşı son imzaları indirebilmelidir.

**2.6.15.13** Teklif edilecek ürün, HTTP ve HTTPS protokolleri ile web trafiğini inceleyebilmeli, ilgili protokollerden gelen objeleri tarayabilmelidir.

**2.6.15.14** Teklif edilerek ürün, oltalama amaçlı yapılmış internet sitelerini bloklayabilmelidir.

**2.6.15.15** Teklif edilerek ürün, henüz bilinmeyen yeni zararlıları davranış tespit özelliği ile tespit edebilmelidir.

**2.6.15.16** Teklif edilerek ürün, uygulamanın hareket ve aksiyonlarını izleyerek anormal davranışları tespit edebilmelidir. Ürün, zararlı yazılım aksiyonlarını geri alabilme yeteneğine sahip olmalıdır (rollback)

**2.6.15.17** Teklif edilerek ürün, belirlenmiş zararlı uygulamaların sistemsel aksiyonlarını engelleyebilmelidir.

**2.6.15.18** Teklif edilecek ürün, uygulamaların kurulumunu ve çalıştırılabilmesini engelleyebilmesine olanak tanımalıdır.

**2.6.15.19** Teklif edilerek ürün, merkezi imza güncellemelerine destek vermeli veya zararlı yazılım imza veritabanının tamamını veya bir kısmını her host'taki güvenlik sanal makinasında tutabilmelidir.

**2.6.15.20** Teklif edilerek ürün, takvim bazlı tarama yapabilmelidir.

**2.6.15.21** Teklif edilecek ürün, zararlı yazılımları zararsız hale getirip silebilmeli ve bu işlemleri yöneticilere bildirim olarak iletebilmelidir.

**2.6.15.22** Teklif edilecek ürün, tüm koruma komponentleri için tek bir yönetim konsolu sunmalıdır.

**2.6.15.23** Teklif edilecek ürün, sanal ve fiziksel makinaların hepsi için tek bir yönetim konsolundan yönetim sunabilmelidir.

**2.6.15.24** Teklif edilecek ürün, sanal makinalardaki olaylar ve koruma görevlerinin çalıştırılması konusunda rapor sunabilmelidir.

**2.6.15.25** Teklif edilecek ürün, farklı gruplardaki sanal makinalara farklı koruma konfigürasyonları uygulayabilmelidir.

**2.6.15.26** Teklif edilecek ürün, sildiği dosyaların yedek kopyalarını da tutabilmelidir.

**2.6.15.27** Teklif edilecek ürün, Live migration, Cluster shared volumes, Dynamic memory, Live backup adlı Microsoft Hyper-V ortam özelliklerini desteklemelidir.

**2.6.15.28** Teklif edilecek ürün, korunacak sunucu sayısı veya sanal makina sayısı veya donanımsal CPU çekirdek sayısına göre lisanslama sağlayabilmelidir.

**2.6.15.29** Teklif edilecek ürün, uygulama çalışma kontrollerini hem Windows masaüstü versiyonlarında hem de Windows sunucu versiyonlarında yapabilmelidir.

**2.6.15.30** Teklif edilecek ürün, belirlenen yoldaki dosyaların değişip değişmediğini anlamak adına "integrity monitoring" komponentini de içermelidir.

**2.6.15.31** Teklif edilecek ürün, ağ bazlı saldırıları tespit etmek ve bloklamak adına bir özelliğe sahip olmalıdır.

**2.6.15.32** Teklif edilecek ürün, zararlı URL'lere erişimin engellenmesi amacıyla WEB koruması özelliğine sahip olmalıdır.

**2.6.15.33** Teklif edilecek ürün, anti-virüs taraması esnasında tüm dosyaları tarayabilmelidir.

**2.6.15.34** Teklif edilecek ürün, koruma modüllerinin tümünü (dosya, web, ağ vs) için tek bir kuraldan (policy) yönetebilmelidir.

**2.6.15.35** Teklif edilecek üründe SIEM entegrasyonu bulunmalıdır.

**2.6.15.36** Teklif edilecek ürün, çalışan uygulamaların davranışlarını izleme özelliğine sahip olmalıdır.

**2.6.15.37** Teklif edilecek ürün, en az 5 yıllık ve ihalede teklif edilen, Merkezde 3 sunucu FKM'de 2 sunucuyu ve 200 sanal sunucuyu kapsayacak şekilde lisanslanmalıdır.

**2.6.15.38** Teklif edilecek ürünün üreticisi, Türkiye'de bizzat üretici firma personeli tarafından Türkçe Teknik destek veren bir ekibe sahip olmalıdır.

**2.6.15.39** Teklif edilecek üründe, üretici firma profesyonel desteği lisanslaması da eklenecektir.

**2.6.15.40** Üretici firma teknik desteği, en az birinci seviyede tamamen Türkçe olarak verilecektir.

**2.6.15.41** Teknik destek çağrı talepleri, 7/24/365 olarak üretici firmaya ait destek portalı üzerinden açılabilmelidir

**2.6.15.42** Teknik destek çağrı talepleri, üretici firmaya ait destek portalındaki kullanıcı hesabında bir problem olması durumunda, 7/24/365 olarak e-posta yoluyla açılabilmelidir

**2.6.15.43** Teknik destek çağrı talepleri, SL1 seviyesinde 7/24/365 olarak, SL2-4 seviyelerinde üretici firma ofisi mesai saatleri içerisinde istenirse telefonla direkt olarak da açılabilmelidir

**2.6.15.44** Teklif edilecek üretici firma teknik destek paketi, aşağıdaki servis seviyelerini sağlamalıdır:

**2.6.15.44.1** L1: 2 saat

**2.6.15.44.2** L2: 6 iş saati

**2.6.15.44.3** L3: 8 iş saati

**2.6.15.44.4** L4: 10 iş saati

**2.6.15.45** Teklif edilecek üretici firma teknik destek paketi sayesinde, firma mevcut teknik destek iş yükü içerisinde kurum taleplerine öncelik sağlamalıdır.

**2.6.15.46** Teklif edilecek üretici firma teknik destek paketinde, 1. seviye yükseltme (escalation) lokal destek ekip müdürüne, 2. seviye yükseltme (escalation) müşteri yöneticisine ve üretici firma bölgesel (regional) ofisine yapılacaktır.

**2.6.15.47** Teklif edilecek üretici firma teknik destek paketi kapsamında müşteri yıllık 36 olay tanımlayabilir.

**2.6.15.48** Teklif edilecek üretici firma teknik destek paketi kapsamında kurum, 4 kontak kişiye kadar yetkili kişi tanımlayabilmelidir.

### 2.6.16 Saldırı Yüzeyi Yönetimi Ürünü

**2.6.16.1** ÜRÜN arayüzüne herhangi bir program/kurulum ihtiyacı olmaksızın web tarayıcı ile (Internet Explorer, Firefox Mozilla, Google Chrome) erişilebilmelidir.

**2.6.16.2** ÜRÜN; güncel tarayıcılarla uyumlu, parola ile giriş sağlanan, SSL destekli, İngilizce web arayüzüne sahip olmalıdır.

**2.6.16.3** ÜRÜN; KURUM'a ait alan adlarını, alt alan adlarını ve IP adreslerini otomatik olarak tespit edebilme yeteneğine sahip olmalıdır.

**2.6.16.4** ÜRÜN; otomatik dijital varlık tespiti kurallarında esneklik imkânı sağlamalıdır.

**2.6.16.5** ÜRÜN; KURUM'a ait alan adı, alt alan adı ve IP adreslerinin manuel girişini desteklemelidir.

**2.6.16.6** ÜRÜN; KURUM'a ait tüm alan adlarını listeleme özelliğine sahip olmalıdır.

**2.6.16.7** ÜRÜN; KURUM'a ait tüm alt alan adlarını listeleme özelliğine sahip olmalıdır.

**2.6.16.8** ÜRÜN; KURUM'a ait tüm IP adreslerini listeleme özelliğine sahip olmalıdır.

**2.6.16.9** ÜRÜN; KURUM'a ait her bir alan adının, alt alan adının ve IP adresinin meta bilgilerini (Whois, DNS, SSL, HTTP) gösterebilmelidir.

**2.6.16.10** ÜRÜN, KURUM'a ait alan adı, alt alan adı ve IP adreslerinde kullanılan web ve network teknolojilerini tespit edebilmelidir.

**2.6.16.11** ÜRÜN; tespit edilen teknolojilerdeki bilinen zafiyetleri listeleyebilmelidir.

**2.6.16.12** ÜRÜN; tespit edilen zafiyetlerle ilgili ayrıntılı bilgi (etki, öncelik, kapsam gibi) sunmalıdır.

**2.6.16.13** ÜRÜN; tespit ettiği her bir güvenlik problemine ait kritiklik seviyesi bilgisi sunmalıdır.

**2.6.16.14** ÜRÜN; tespit ettiği her bir güvenlik problemine dair çözüm önerisi sunmalıdır.

**2.6.16.15** ÜRÜN; KURUM'a ait dijital varlıklarda kullanılan tüm teknolojileri, versiyonları ve versiyonlardaki güvenlik zafiyetlerini tek bir sayfa üzerinde gösterebilmelidir.

**2.6.16.16** ÜRÜN; KURUM'a ait dijital varlıkların DNS bilgilerini takip ederek herhangi bir değişiklikte ve güvenlik problemi ihtimalinde bildirimde bulunmalıdır.

**2.6.16.17** ÜRÜN; KURUM'a ait dijital varlıkların SSL sertifika bilgilerini panel üzerinde göstermeli, bu bilgileri takip ederek herhangi bir güvenlik problemi ihtimalinde ve SSL sertifikasının süresi bitmeden önce bildirimde bulunmalıdır. ÜRÜN'ün bu bildirimleri otomatik olarak yapamadığı durumda, görevi YÜKLENİCİ üstlenerek KURUM'a gerekli bildirimi yapacaktır.

**2.6.16.18** ÜRÜN; KURUM'a ait dijital varlıklardaki tüm güvenlik problemlerini tek bir sayfa üzerinden sunabilmelidir.

**2.6.16.19** ÜRÜN; sunduğu veriler üzerinden filtreleme ve arama özelliği sunmalıdır.

**2.6.16.20** ÜRÜN; KURUM saldırı yüzeyine ait özet bilgileri içeren PDF formatında yönetici raporu alma özelliği sunmalıdır.

**2.6.16.21** ÜRÜN; KURUM'a ait her bir dijital varlığın saldırı yüzeyi ve güvenlik problemlerine dair detaylı PDF veya CSV raporu alma özelliği sunmalıdır.

**2.6.16.22** ÜRÜN; yüz kullanıcıya kadar hesap açılmasını desteklemelidir.

**2.6.16.23** ÜRÜN; kullanıcı giriş-çıkış ve işlem loglarını tutabilmelidir.

**2.6.16.24** ÜRÜN; web arayüzü üzerinden kullanıcılardan geri bildirim alabilmelidir.

**2.6.16.25** ÜRÜN; API (Uygulama Programlama Arabirimi) desteği sunmalıdır.

**2.6.16.26** ÜRÜN; zengin ve kolay geliştirilebilir entegrasyona sahip API'ler sunabilmelidir. API üzerinden paylaşılan veri formatı JSON veya CSV formatlarını desteklemelidir.

**2.6.16.27** ÜRÜN; API üzerinden gelişmiş filtreleme ile istek atılmasına olanak sağlamalıdır.

**2.6.16.28** YÜKLENİCİ; ÜRÜN'e %99 erişilebilirliği garanti etmelidir.

**2.6.16.29** YÜKLENİCİ; ÜRÜN ile ilgili detaylı API dokümanı sağlamalıdır.

**2.6.16.30** YÜKLENİCİ; bir yıl boyunca ÜRÜN'de yapılacak tüm güncelleme ve versiyon değişikliklerinde oluşan/değişen dokümanları her seferinde elektronik ortamda KURUM'a teslim etmelidir.

**2.6.16.31** YÜKLENİCİ, KURUM'dan gelecek talep doğrultusunda işbu şartname ile satın alınan ÜRÜN'e ilişkin olarak web ekranlarının kullanımına yönelik yılda iki kezle sınırlı olmak üzere kullanıcı eğitimlerini vermelidir.

**2.6.16.32** YÜKLENİCİ, KURUM'dan gelecek talep doğrultusunda API kullanımına ilişkin Python dilinde hazırlanmış örnek kodlar paylaşmalıdır.

**2.6.16.33** YÜKLENİCİ; KURUM tarafından e-posta üzerinden iletilen destek taleplerine en geç 24 saat içinde cevap vermelidir.

**2.6.16.34** Bu şartname, KURUM'a ait en az bin (1000) dijital varlığın 30 gün süre ile tespit edilip taranmasına imkân sağlayacak şekilde en az 5 (beş) yıl süreli lisans ile teklif edilecektir.

### 2.6.17 Sanallaştırma Yazılımı

**2.6.17.1** Bu şartnamedeki koşulları karşılayan sanallaştırılmış altyapı alınacaktır.

**2.6.17.2** Teklif veren firma ürünleri satmaya yetkili olduğunu üreticinin Türkiye temsilcisi veya yetkili distribütörü tarafından verilmiş yetki belgesi ile ispatlayacaktır.

**2.6.17.3** Aşağıda belirtilen yazılımlar ihalede teklif edilen, Merkezde 3 sunucu FKM'de 2 sunucunun, bütün CPU (işlemci), Core (çekirdek) ve RAM (bellek) kaynaklarını kullanabilecek özellikte ve sanal sunucu sayısı limiti olmaksızın lisanslamaya sahip olacak ve gerekli lisanslar teklif edilecektir.

**2.6.17.4** Bu şartnamedeki tüm maddeler aynı üreticiye ait olan ürünlerden sağlanacaktır.

**2.6.17.5** Teklif edilen yazılım lisansları farklı marka ve model fiziksel sunucular arasında taşınabilir ve bölünebilir olmalıdır. Teklif edilen yazılımlar için, yazılım üreticisinin destek merkezine herhangi bir aracıya ihtiyaç duymadan direk çağrı açılabilecektir.

**2.6.17.6** Sanallaştırma yazılımı, işletim sisteminden bağımsız ve kernel seviyesinde çalışan sanallaştırma (hypervisor) katmanına sahip olmalıdır.

**2.6.17.7** Sanallaştırma yazılımı, sanal SMP (Symmetric Multi-Processing) destekli olmalı ve sanal makinalara birden fazla sanal CPU tanımlanabilmesine olanak sağlamalıdır.

**2.6.17.8** Sanallaştırma yazılımı, sunucularda kurulu olan sanallaştırma katmanını güncelleyebilecek, yamalarını yapabilecek ve üst sürümlere yükseltebilecek entegre bir güncelleme modülü içermelidir.

**2.6.17.9** Sanallaştırma yazılımı, ortak depolama alanından tanımlanmış bir LUN üzerine birden fazla sunucunun aynı anda okuma ve yazma yapmasına olanak sağlayan aktif-aktif dosya sistemine sahip olmalıdır.

**2.6.17.10** Sanallaştırma yazılımı, herhangi bir fiziksel sunucu arızası söz konusu olduğunda ya da sanal sunucu üzerindeki ajandan haber alamadığı durumda, o sunucunun üzerinde çalışan sanal makinaları ortamdaki diğer fiziksel sunucular üzerinde tekrar çalıştırabilmelidir. Bu yapıda, sanal makinalar için önceliklendirme yapılabilmelidir.

**2.6.17.11** Sanallaştırma yazılımı, SAN, yazılımsal/donanımsal iSCSI ve NFS protokollerini kullanan veri depolama sistemlerini desteklemeli ve bu protokolleri kullanarak sisteme disk tanımlaması yapılabilmelidir.

**2.6.17.12** Sanallaştırma yazılımı, sanal makinaların verilerinin bulunduğu disk alanının herhangi bir kesinti olmadan büyütülebilmesine olanak sağlamalıdır.

**2.6.17.13** Sanallaştırma yazılımı, sanal makinalarda disk sanallaştırması (thin provisioning) destekli disk tanımlamalarına olanak sağlamalıdır.

**2.6.17.14** Sanallaştırma yazılımı, yaratılan sanal makinaların (lokal diskte ya da ortak depolama alanında) ihtiyaç duyulduğunda çalışmaları durdurulmadan ve herhangi bir veri kaybı olmadan sistemdeki diğer bir fiziksel sunucu üzerine taşınabilmelerine olanak sağlamalıdır. Bu işlem farklı yönetim yazılımları arasında da desteklenmelidir.

**2.6.17.15** Sanallaştırma yazılımı, sanal makinalar çalışır durumda iken işlemci, bellek, disk ve ağ adaptörü eklenmesine olanak sağlamalıdır.

**2.6.17.16** Sanallaştırma yazılımı, misafir işletim sistemi (Guest OS) olarak Windows 8/10, Windows Server 2016/2019, Ubuntu Server, SUSE Linux, Redhat Ent.Linux 6/7, Sun Solaris 11, CentOS, FreeBSD, Debian, Oracle Linux ve Mac OS X Server işletim sistemlerini desteklemelidir.

**2.6.17.17** Sanallaştırma yazılımı istendiğinde entegre bir çözüm kullanılarak iş sürekliliği (sanal makinaların bir plan doğrultusunda farklı bir lokasyonda çalıştırılması) çözümüne sahip olacaktır.

**2.6.17.18** Sanallaştırma yazılımı, tüm sanal altyapıyı yönetebilecek sanallaştırma yönetim yazılımı içermelidir.

**2.6.17.19** Sanallaştırma yönetim yazılımı, kullanıcı yetkilendirmesi özelliğine sahip olacaktır. Farklı kullanıcılar için farklı yetkilendirmeler ve haklar tanımlanabilecektir.

**2.6.17.20** Sanallaştırma yönetim yazılımı hem fiziksel sunucuların hem de sanal makinelerin kaynak kullanımlarını anlık ya da geriye dönük raporlayabilme özelliğine sahip olacaktır.

**2.6.17.21** Sanallaştırma yönetim yazılımı, üreticisi tarafından sağlanan sanal appliance (hazır sanal makina) şeklinde kullanılacaktır.

**2.6.17.22** Sanallaştırma yönetim yazılımı, tüm sistemin web ara yüzünden yönetilmesine olanak sağlayacak modüle sahip olacaktır.

**2.6.17.23** Teklif edilecek tüm sanallaştırma yazılımlar 5 yıllık destek paketi içermelidir.

**2.6.17.24** Destek paketi ile yazılım üreticisinin destek merkezine herhangi bir aracıya ihtiyaç duymadan direk çağrı açılabilecektir.

**2.6.17.25** Teklif edilen sanallaştırma yazılımlarının kurulumu, üreticisi tarafından veya üretici tarafından yetkilendirilmiş servis bayisi tarafından gerçekleştirilecektir.

**2.6.17.26** Sanallaştırma yazılımları destek paketinin geçerli olduğu süre boyunca yazılım ürünlerinin yeni çıkan sürümleri ücretsiz olarak sağlanacaktır.

### 2.6.18 Yedekleme Yazılımı

**2.6.18.1** Yazılım için destek alınabilmeli ve yeni çıkan sürümler yüklenebilmelidir ve lisans kalıcı ya da abonelik olarak kullanılmalıdır.

**2.6.18.2** Yazılım, Merkezde bulunan 3 sunucuyu (6 CPU'yu) lisanslamalıdır. Yazılım lisanslaması Instance ya da CPU socket temelli olmalıdır. Instance temelli lisanslama olursa en az 100 instance için lisanslama yapılmalıdır.

**2.6.18.3** Yazılım VMware vSphere (4.x, 5.x, 6.x 7 and 8.0), Microsoft Hyper-V (2012, 2012R2, 2016, 2019,2022), sanallaştırma platformlarında çalışan sanal makinaların yedeklemesini, iş sürekliliğini, proaktif olarak izlenmesini ve raporlanmasını sağlayarak, imaj seviyesinde ve uygulama tutarlı olarak yapabilmelidir.

**2.6.18.4** Yazılım, yedekleri saklamak için Windows, Linux FC-SAN, IP-SAN, NFS, CIFS, LVM dosya paylaşımlarını ve üzerinde dahili tekilleştirme sunan cihazları kullanabilmelidir.

**2.6.18.5** Yazılım tanımlanmış 3 farklı yedekleme deposunu tek bir 'büyütülebilen yedek deposu' olarak kullanarak disk alanı yönetimini basitleştirmelidir.

**2.6.18.6** Yazılım bir yedekleme görevi içindeki her sanal makina için ayrı ayrı tam ve artımlı dosya zincirleri oluşturabilmelidir.

**2.6.18.7** Yazılım herhangi bir ajan kurulumu gerektirmeden kullanıcı tarafından özelleştirilebilen veya devre dışı bırakılabilen dahili sıkıştırma ve tekilleştirme sunmalıdır.

**2.6.18.8** Yazılım artımlı yedekler için hipervizörlerin sunduğu Değişen Blok Takibi (CBT) özelliğini kullanmalıdır.

**2.6.18.9** Yazılım yedeklerin saklandığı diskte bulunan tam ve artımlı yedekleri kullanarak yeni tam yedekler oluşturabilmelidir.

**2.6.18.10** Yazılım ile yedeklenmesi istenmeyen sanal diskler ile NTFS dosya sistemlerindeki dosya ve klasörler seçilerek; geçici dosyalar ve silinmiş öğelere ait disk blokları tespit edilerek yedekleme ve artırımlı işlemi dışında bırakılabilmelidir.

**2.6.18.11** Yazılım yedekleme ve artırımlı için sanal makina verisini doğrudan Veri Depolama ağı üzerinden, Ağ üzerinden veya Hipervizör I/O platformu üzerinden aktarma seçenekleri sunmalıdır.

**2.6.18.12** Yazılım NFS disk alanlarına direkt erişerek yedekleme ve kurtarma işlerini hızlandıracak Vmware NFS 3 ve 4.1 destekli bir istemci sunmalıdır.

**2.6.18.13** Yazılım saklanan yedekleri ve ağ trafiğini uçtan uca (kaynakta, aktarırken ve depolarken) AES256bit şifreleyebilmeli ve kayıp şifre koruması sunmalıdır.

**2.6.18.14** Yazılım görevlerin kullanabileceği network bant genişliğini, eş zamanlı çalışacak görev sayısını, backup diskine aynı anda yazılabilecek kanal sayısı ve veri oranını yöneticinin istediği değerlerde limitleyebilmelidir.

**2.6.18.15** Yazılım kaynak Sanal Makinaların bulunduğu disk alanılarındaki I/O gecikmelerini izleyebilmeli ve kullanıcı tarafından belirtilen değer aşıldığında o disk alanı üzerinde bir yedekleme veya artırım görevi başlatmamalı ve çalışan ortam performansının olumsuz etkilenmesi engellenmelidir.

**2.6.18.16** Yazılım üretici onaylı bir bulut servis sağlayıcı tarafından sunulan Bulut üzerinde disk hizmetini, yedeklerin saklanacağı bir yedek deposu olarak tanımlayabilmeli, yedeklerini veya yedek kopyalarını bu alana gönderebilmelidir.

**2.6.18.17** Yazılım Microsoft SQL, Oracle, Oracle Rack, MySQL, PostgreSQL yedekleme ve geri yükleme özellikleriyle hem fiziksel hem de sanal makinelerde veritabanları desteklemelidir

**2.6.18.18** Yazılım bir sanal makinayı tam veya artımlı yedek dosyasından orjinal yerine veya başka bir ana sunucu üzerine geri yükleyebilmelidir.

**2.6.18.19** Yazılım bir sanal makinayı yedekten geri yüklerken sadece değişen blokları kullanarak kurtarma yapabilmelidir.

**2.6.18.20** Yazılım bir sanal makinanın sadece ana sunucu üzerindeki dosyalarını geri yükleyebilmelidir.

**2.6.18.21** Yazılım bir sanal makinanın sadece seçilen sanal disklerini geri yükleyebilmelidir.

**2.6.18.22** Yazılım geçerli bulut hizmetleri abonelik bilgileri sağlandığında, bir sanal makinayı doğrudan Microsoft Azure veya AWS, Open Stack, ortamına geri yükleyebilmelidir.

**2.6.18.23** Yazılım, destekleyen Linux işletim sistemleri üzerindeki diskler ile, sabit (immutable) yedekleme havuzu oluşturabilmeli ve hızlı blok klonlama yeteneği bulunmalıdır

**2.6.18.24** Yazılım sanal makinaya herhangi bir ajan/servis kurulumu gerektirmeden, sanallaştırma platformunun desteklediği tüm işletim sistemlerinden, sunucunun tamamını geri yüklemeye gerek kalmadan sadece istenilen klasör veya dosyaları arama, bulma, dışa aktarma ve geri yüklemesini yapabilmelidir.

**2.6.18.25** Yazılımın Web uygulaması kullanılarak yedekler içerisinden Sanal Makinaların ve Dosyaların geri yüklemesi yapılabilmelidir.

**2.6.18.26** Yazılım vSphere Web Client'a entegre olabilmeli, anlık hızlı yedeklemeler buradan başlatılabilmeli, yedeklerin ve yedekleme kaynaklarının durumları, yedeklerin saklandığı disklerin boş/dolu alan bilgileri, korunan sanal makinalar gibi bilgilere doğrudan web client içerisinden erişilebilmelidir.

**2.6.18.27** Yazılım kendi konfigurasyon yedeğini herhangi bir kullanıcı müdahalesi gerekmeden tanımlı disk alanına alabilmeli ve tüm ayarları ve tanımlamaları içerecek şekilde geri yüklenebilmelidir.

**2.6.18.28** Uzak ofislerde ve uç noktalarda yedekleme ve kurtarma işlemleri için uzak nokta etkileşim proksi sunucusu ve yükleme sunucuları kullanılabilmelidir.

**2.6.18.29** Yazılım dahili komut satırı (WebSSH) Desteği sunmalıdır.

**2.6.18.30** Yazılım, geçmişe dönük performans ve alarm verilerinin saklanması için gerekli veritabanını kurulum esnasında otomatik olarak yüklemelidir.

**2.6.18.31** Yazılımın konsol, veritabanı ve web sunucusu bileşenleri aynı sunucu üzerine veya yapının büyüklüğüne göre farklı sunucular üzerine kurulabilmelidir.

**2.6.18.32** Yazılım vmware ortamlarında vcenter üzerinde tanımlanmış kullanıcı erişimlerine göre kullanıcılara sadece yetkileri olan bölümlerde izleme ve raporlama sunabilmelidir.

**2.6.18.33** Yazılım, Microsoft Windows tabanlı sanal makinaların işletim sistemlerine ayrı bir araç ile ulaşmaya gerek kalmadan yürüttüğü işlemleri görüntülemeli, yönetmeli ve konsol erişim sağlamalıdır.

**2.6.18.34** Yazılım, disk hacmi, disk sorunları, disk alanı kullanımı, veri deposu görüntüleme de dahil tam bir veri depolama görüntülemesi sağlamalıdır.

**2.6.18.35** Yazılım sanallaştırma altyapı bileşenleri ile ilgili önceden tanımlanmış, kategorize edilmiş ve kurulum tamamlandığında kullanıcı müdahalesi gerektirmeden çalışmaya başlanan hazır alarmlar sunmalıdır.

**2.6.18.36** Yazılım, sanallaştırma sunucusu, sanal makinalar ve veri depolarında oluşabilecek sorun ve darboğazları tespit edip alarmlar üretmeli, önceden tanımlanmış kişi ve gruplara e-posta olarak iletebilmeli ve tanımlanmış programları çalıştırmalıdır.

**2.6.18.37** Yazılım içerisindeki tüm raporlar istenilen sıklıkta zamanlanarak ilgili kişi veya gruplara, paylaşım ve portallere otomatik olarak gönderilebilmelidir.

**2.6.18.38** Yazılım sanallaştırma sunucusu ve sanal makinaların kaynak kullanımını tanımlanan gruplara göre raporlama ve ücretlendirme yapmalıdır.

**2.6.18.39** Yazılım, Yedekleme altyapısının bileşenleri için gerçek zamanlı izleme sunmalıdır.

**2.6.18.40** Yazılım, Yedekleme altyapısının bilşenleri için kullanım ve kapasite planlama raporları sunmalıdır.

**2.6.18.41** Yazılım, sanal altyapıda bulunan tüm sanal makinalar için, bu sunucuların ilk ve son yedeklenme tarihlerini, geri dönüş nokta sayılarını, hangi görev içinde korunduklarını içeren kapsamlı bir korunma raporu sunabilmelidir.

**2.6.18.42** Sanal Altyapı içerisindeki her öğe ile ilgili tüm raporlara ayrı bir arayüze gerek olmaksızın doğrudan konsol içerisinden erişim sağlanabilmelidir.

**2.6.18.43** Yazılım sanal altyapı içerisindeki sanal makinaları, sağlıklı yedeklemeyi engelleyecek (disk boyutu, açık snapshot, vmware veya hyperv araçlarının güncelliği vb) faktörleri denetleyerek uygun olmayanları raporlayabilmelidir.

**2.6.18.44** Yazılım, sanal sunucularda günlük değişen veri miktarını hesaplayarak yedekleme alanı hesaplarında kullanılmak üzere raporlayabilmelidir.

**2.6.18.45** Teklif edilen yedekleme yazılımı CDP (Continuous Data Protection) özelliği desteği olmalıdır.

**2.6.18.46** Yazılımın lisanslaması korunmakta (yedeklenmekte ve/veya replike edilmekte) ve izlenip raporlanmakta olan sanal makinaları çalıştıran ana sunucuların fiziksel işlemcisi bazında olmalı ve en fazla 7 fiziksel sunucu 5 yıl kalıcı lisans sahip, ve üreticin sunmuş olduğu versiyon yükseltme paketiyle işlemciye kadar olan ortamları destekleyecek lisanslama modeli ve 7x24 en yüksek destek paketini sunulmalıdır.

### 2.6.19 Sunucu İşletim Sistemi

**2.6.19.1** Yazılım 14 soket işlemcisi olan ve toplam işlemcisi 144 Çekirdek olan 7 adet sunucuyu lisanslayabilmelidir. Fiziksel sunucular üstünde kurulabilecek sanal işletim sistemi sayısında bir sınır olmamalıdır.

**2.6.19.2** Sunucu işletim sistemi sanallaştırma teknolojisi içermeli ve lisanslanan donanımlar üzerindeki sanal sunucuların lisanslarını da ihtiva etmelidir.

**2.6.19.3** Sunucu işletim sistemi sanal sunucular için replikasyon teknolojisi içermeli ve bu sayede felaketten kurtarma altyapıları oluşturulabilmelidir.

**2.6.19.4** Sunucu işletim sistemi lokal disk alanlarını veri depolama alanları şeklinde diğer sunucuların hizmetine açabilmelidir.

**2.6.19.5** Sunucu işletim sistemi disk alanlarındaki verilerin tekilleştirilmesini desteklemeli ve bu sayede veri alanı maliyetlerini düşürebilmelidir.

**2.6.19.6** Sunucu işletim sistemi çekirdek kurulum veya grafiksel kurulum seçeneği sunabilmeli, istenildiği zaman grafiksel veya çekirdek kurulum arasında geçiş yapılabilmelidir. Grafiksel arayüz veya komut satırı üzerinden sistemin yönetimi mümkün olmalıdır.

**2.6.19.7** Sunucu işletim sistem ağ kartlarını takım olarak kullanabilmeli ve bu sayede daha yüksek bant genişliği, yüksek erişilebilirlik sağlayabilmelidir. Bu özellik için donanım üreticilerinin ek yazılımlarına ihtiyaç duyulmamalıdır.

**2.6.19.8** Sunucu işletim sistemi fiziksel makine başına 320 işlemci ve 4 TB bellek desteklemelidir.

**2.6.19.9** Sanal sunucu başına 64 vCPU ve 1 TB bellek desteklenmelidir.

**2.6.19.10** Sanal sunuculara 64TB boyutunda sanal diskler eklenebilmelidir.

**2.6.19.11** Sunucu işletim sistemi kümeleme yöntemiyle yüksek erişilebilirlik desteklemelidir. Yüksek erişilebilir sunucu havuzları 64 ayrı sunucudan oluşabilmelidir.

**2.6.19.12** Sanal sunuculara vHBA sürücüleri yüklenebilmeli. Gerektiğinde fiber depolama alanlarındaki LUN yapıları sanal sunuculara direk olarak atanabilmelidir.

**2.6.19.13** Önerilen OS LDAP v3 Active Directory'ler ile uyumlu çalışabilmelidir.

**2.6.19.14** Kerberos v5 authentication protocol desteği olmalıdır.

**2.6.19.15** İstemci makineler üzerinde politikalar uygulanabilmelidir.

**2.6.19.16** Federasyon servisleri desteklenmelidir.

**2.6.19.17** Tek bir domain içinde birden fazla şifre politikası ayarlanabilmelidir.

**2.6.19.18** Şube kurulumları için salt okunabilir dizin servisleri bulunmalıdır.

**2.6.19.19** Dizin servisleri dosya ve epostalar için hak yönetimi yapabilmelidir.

**2.6.19.20** Önerilen OS içinde dış saldırılardan korunabilmek için bir firewall özelliği olmalıdır.

**2.6.19.21** Firewall özelliği hem işletim sisteminden dışarı hem de dışarıdan işletim sistemine olan bağlantıları kontrol edebilmelidir.

**2.6.19.22** İşletim sistemi donanım tabanlı şifreleme yaparak disk üzerindeki her türlü bilgiyi şifreli olarak tutabilmelidir.

**2.6.19.23** Kurumsal ağa, VPN, IPSEC, DHCP veya 802.1X ile bağlanan işletim sistemlerini kontrol edebilmeli ve işletim sistemleri sağlıklı ise kurumsal ağa almalı, eğer sağlıklı değil iseler karantina bölgesine almalıdır.

**2.6.19.24** Önerilen OS içinde entegre PKI yapısı olmalı, bir Certificate Authority (CA) olarak davranabilmeli ve bunun için ek bir maliyete gerek duyulmamalıdır.

**2.6.19.25** Certificate Authority (CA), OCSP (Online Certificate Status Protocol) desteğine sahip olmalıdır.

**2.6.19.26** Certificate Authority (CA), Network cihazları için kaydetme (enrollment) servisine sahip olmalıdır.

**2.6.19.27** Smartcard desteği OS içinde gelmelidir. Önerilen OS, TCP/IP seviyesinde gelen yükü farklı makinalar arasında paylaştırabilmelidir.

**2.6.19.28** Bu paylaşımı kurallara bağlı olarak port ve IP bazında yapabilmelidir.

**2.6.19.29** Birden fazla NIC desteği olmalı ve bunlar arasında bi-directional affinity ile yük paylaşımı yapabilmelidir.

**2.6.19.30** VPN ve RAS servisleri ücretsiz olarak OS ile gelmelidir.

**2.6.19.31** Önerilen OS, IPv6 protokolünü desteklemelidir.

**2.6.19.32** Önerilen OS, içinde VPN hizmetleri gelmelidir

**2.6.19.33** Önerilen OS, içinde RADIUS hizmetleri olmalıdır.

**2.6.19.34** Önerilen OS, üzerindeki network kartları arasında bridging yapabilmelidir.

**2.6.19.35** Önerilen OS, NAT ve ICF özelliklerine sahip olmalıdır.

**2.6.19.36** Internet connection sharing desteği olmalıdır.

**2.6.19.37** Önerilecek işletim sistemi üzerinde ASP.NET uygulamalarının çalışabilmesi için gerekli olan .NET Framework 1.1 bulunmalıdır servisleri için gerekli olan UDDI hizmetini sunabilmelidir.

**2.6.19.38** ASP ve ASP.NET uygulamalarını desteklemelidir.

**2.6.19.39** Web sunucusu tüm konfigürasyonunu XML olarak tutmalı ve bu dosya üzerinde yapılacak değişiklikler anında sisteme yansımalıdır.

**2.6.19.40** XML Web

### 2.6.20 Sunucu İşletim Sistemi Erişim Lisansı

**2.6.20.1** Sunucu işletim sistemi lisansları, 400 kullanıcı için kullanıcı erişim lisansıyla birlikte teklif edilmelidir.

### 2.6.21 E-Posta Sunucusu

**2.6.21.1** E posta sisteminin çoklu işlemci desteği olmalıdır.

**2.6.21.2** E posta sistemi asgari 6 posta kutusu veri tabanı sistemini desteklemelidir.

**2.6.21.3** E posta sisteminin yüksek erişilebilirlik desteği sağlayabilmesi için 3 Merkez, 2 adet FKM için ürün kurulumu yapılmalıdır.

**2.6.21.4** Tüm sunucular tamamen merkezi olarak yönetilmelidir.

**2.6.21.5** Eposta sistemi konsolidasyon (sayılarının azaltılarak konsantrasyon merkezine toplanabilmesi) senaryolarını desteklemelidir.

**2.6.21.6** Eposta sistemi web tabanlı ersişimi ve POP3, IMAP4, MAPI, HTTP, WAP2.0 kullanan istemci modellerini desteklemelidir.

**2.6.21.7** Mobil cihazlardan ek bir yazılıma gerek duymadan erişimi desteklemeli, bu cihazlardan Eposta, Takvim ve Kontak bilgileri otomatik senkronize edilebilmelidir.

**2.6.21.8** Ek bir yazılıma gerek duymadan cep telefonlarından ulaşılarak metin tabanlı Eposta görüntülenebilmelidir.

**2.6.21.9** Ön-plan ve Arka-plan Sunucu mimarisini desteklemeli, ön-plan sunucu NLB (Network Load Balancing) ile yük dağılımı yapabilmelidir.

**2.6.21.10** Laptop kullanıcıları Eposta sisteminin DMZ bölgesinde bir ön plan sunucusu olmasa da arka-plan sunucusuna güvenli bir şekilde erişmeli ve epostalarını şirket içerisinde çalışıyormuş gibi yerel diskine indirebilmelidir.

**2.6.21.11** SAN (Storage Area Network) yapısını desteklemeli ve bu yapıda kullanılabilecek Anlık Görüntü (snapshot) alabilme teknolojilerini kendi Eposta yazılımı ile bütünleşik kullanabilmelidir.

**2.6.21.12** İnternetten ulaşılabilir bir "web mail" yapısına sahip bir istemcisi olmalı, bu yapıda istemcinin bağlantı hızına bağlı olarak düşük bant genişliğinde hızlı çalışabilecek bir seçeneği olmalıdır.

**2.6.21.13** Web e-posta istemcisi sayısal imza, SSL ve sunucu tarafı kurallarını desteklemelidir.

**2.6.21.14** Web e-posta istemcisi Smart Card kullanımını desteklemelidir.

**2.6.21.15** Web e-posta ürününü sürekli güncellenen ve yeni teknolojiler ile bütünleşik çalışabilir yapıda olmalıdır.

**2.6.21.16** Eposta sisteminin LDAP desteği olmalıdır.

**2.6.21.17** Microsoft Active Directory yapısı ile bütünleşik çalışabilmelidir.

**2.6.21.18** Eposta sistemi ve web e-posta istemcisi üzerinde gerek firma içi gerekse firma dışı mesajlaşma sırasında virüs kontrolü yapılabilmelidir.

**2.6.21.19** Eposta sistemi kolay yedeklenebilir ve hata oluşması durumunda kısa sürede kurtarılabilir olmalıdır.

**2.6.21.20** Eposta sistemi ve web e-posta istemcisinin Türkçe desteğinin olmalıdır.

**2.6.21.21** Eposta sistemi ve web e-posta istemcisi doğal (native) SMTP yönlendirme (routing) yapabilmelidir.

**2.6.21.22** Posta yoğunluğunun artması durumunda yük dağılımı yapılabilmelidir

**2.6.21.23** Eposta sistemi yedekli çalışma yeteneğine sahip olmalıdır.

**2.6.21.24** Eposta sistemi 2, 4 ve 8 düğümlü kümeleme desteklemelidir.

**2.6.21.25** Eposta sistemi kullanılarak tüm kullanıcılara mesaj gönderilebilmeli ve bu işlem için gerekli kullanıcı haklarının düzenlenebilmelidir.

**2.6.21.26** Eposta sistemi ve istemcisi içerik kontrolü yapabilmeli ya da içerik kontrolü yapabilen ürünler ile entegre çalışabilmelidir (Content Checking, SPAM, Bulk Mail)

**2.6.21.27** Sistemin ortak olarak kullanılabilecek takvim özelliğinin olmalıdır

**2.6.21.28** Kişiler ya da gruplar arası yönlendirilebilen ve yapılacak işlerin kaydedilebileceği bir mekanizmanın olmalıdır. Kaydedilen işler ile ilgili alarm oluşturulabilmelidir (To Do List)

**2.6.21.29** Kullanıcılar e-posta sistemini kullanırken mouse'u kullanarak sürükle/bırak özelliği kullanabilmelidir. (Drag & Drop)

**2.6.21.30** Kullanıcılar web browser üzerinden eriştiği mail ortamındaki inbox, sent, draft, trash gibi dizinlere erişebilmeli ve kendi dizin yapısını oluşturabilmelidir.

**2.6.21.31** Kullanıcılar Eposta gönderimi sırasında öncelik belirtilebilmelidir (Delivery priority)

**2.6.21.32** Gönderilen epostanın özel olarak şifrelenmeli ya da imzalanabilmelidir. (Encryption, Signature)

**2.6.21.33** İstenildiğinde gönderilen epostanın kopyalanmasının, yazdırılmasının, bir başka sunucuya iletilmesinin engellenmesi teknolojilerini desteklemelidir.

**2.6.21.34** İstenildiğinde gönderilen epostanın sadece erişimine izin verilen kullanıcılar tarafından açılması teknolojileri desteklenmelidir.

**2.6.21.35** Kullanıcıların merkezi eposta sistemi ile bağlantıları kopması durumunda da eposta işlevlerini yerine getirebilmesini sağlamalıdır (Offline Service)

**2.6.21.36** Dağıtım listelerini kimlik doğrulamasından geçmiş kullanıcılar ile sınırlama desteği olmalıdır.

**2.6.21.37** Gerçek Zamanlı Güvenli ve Engellenecekler listesi desteği olmalıdır.

**2.6.21.38** Dahili alıcı filtrelemesi yani gelen mesajları alıcıya göre filtreleyebilir ve istenmeyen eposta mesajları azaltabilme desteği olmalıdır.

**2.6.21.39** Kullanıcılar eposta arabirimini kullanarak şifresini değiştirebilmelidir.

**2.6.21.40** Kullanıcı epostaları için eposta sistem yöneticisinin kota uygulayabilmelidir. Kotalar gruplara ya da kullanıcılara göre farklı koşullarda sağlanabilmelidir.

**2.6.21.41** Eposta sistemi veritabanında epostaları Single Instance Storage özelliğinde tutmalıdır.

**2.6.21.42** E-Posta sisteminin zaman planlama yardımcısı (scheduling assistant) olmalıdır. Zaman planlama yardımcısı, toplantı ve kaynak organize etmek isteyen kullanıcıya, en iyi zaman ve tarihleri, katılımcılar ve kaynakların zaman planlarına göre görsel olarak sunabilmelidir.

**2.6.21.43** Sistem, üzerinde organize edilen toplantı taleplerinde değişiklik olduğunda, tekrar bir uyarı göndermeye gerek bırakmamalı, tüm operasyonlar sunucu üzerinde gerçekleşebilmeli ve son kullanıcı toplantılarla ilgili güncellemeleri almak için istemcisini açık tutmak zorunda kalmamalıdır.

**2.6.21.44** Toplantı için kullanılacak odalar ve ekipman, adres defteri içinde özel olarak işaretlenmiş olmalı, böylece bu kaynaklar, ayrı olarak izlenebilir ve bunlara özel yetkiler ve özellikler atanabilmelidir.

**2.6.21.45** Ofis Dışında mesajlarının otomatik olarak gönderileceği başlangıç ve bitiş tarihleri belirlenebilmelidir. İç ve dış alıcılar için farklı mesajlar belirlenebilmelidir.

**2.6.21.46** Posta kutuları, default olarak tamamen indekslenmiş olmalı ve sistem tarafından hızlı ve güvenilir bir arama altyapısı sunulmalıdır.

**2.6.21.47** Sistem, web tabanlı bir erişim sunmalıdır. Web tabanlı erişimde zaman planlama asistanı, kategoriler ve bayraklar ve arama özellikleri kullanılabilmelidir.

**2.6.21.48** Web tabanlı erişimde Word, Excel, Powerpoint ve PDF dokümanları, istemcide bu dokümanları açacak editör olmasa bile, HTML'e çevrilip görüntülenebilmelidir. Belgelerin sadece HTML olarak görüntülenebilmesi sağlanabilmelidir.

**2.6.21.49** Bir kullanıcı bir dosya paylaşımını işaret eden link aldığında, sistem VPN'e gerek bırakmadan güvenli bir şekilde kullanıcının bu dosyaya ulaşımına ve kullanımına izin vermelidir.

**2.6.21.50** İstemci tarafındaki caching mekanizması, düşük hızlı bağlantılarda gelişmiş bir kullanıcı deneyimi sağlamalı ve bant genişliği kullanımını düşürmelidir.

**2.6.21.51** Sistem elektronik postaları, sesli postaları, takvim öğelerini ve faksları kullanıcının posta kutusuna gönderebilmelidir. Böylece son kullanıcının üretkenliği, ortak tipteki iletişim kanallarının tek bir yerde toplanmasıyla artmalıdır.

**2.6.21.52** Sistem telefonlara yanıt verebilmeli ve kullanıcı çağrıyı cevaplamadığında ya da meşgul olduğunda sesli mesaj kaydedebilmelidir.

**2.6.21.53** Sistemin faks alma yetenekleri, bir faks çağrısına cevap vermeyi, bir faks almayı ve bunu kullanıcının posta kutusuna göndermeyi sağlamalıdır.

**2.6.21.54** Sistemin sesli posta yeteneklerine erişim için kullanılan bir PIN kodu bulunmalı, kullanıcılar PC tabanlı ya da Web tabanlı istemcilerini kullanarak bu sesli posta PIN kodlarını resetleyebilmelidirler. Böylece çağrı merkezi isteklerinin büyük bölümünün düşmesi sağlanmalıdır.

**2.6.21.55** Sistem, İngilizce ses tanıma özellikleri sağlamalı ve arayanların sesle şirket dizinine ulaşıp istedikleri kontağa ulaşabilmeleri sağlanabilmelidir.

**2.6.21.56** Kullanıcılar posta kutularına herhangi bir telefon ile ulaşabilmeli, elektronik posta ve takvimlerini dinleyip, bunlar üzerinde ister sesle ister tuşlama ile aksiyon alabilmelidirler.

**2.6.21.57** Sistem, sağlayıcı şirketin anlık mesajlaşma ve iletişim çözümüyle entegre çalışmalı, sistemin istemcisi üzerinden, kullanıcıların varlık bildirimleri (presence) görünüyor olmalı ve kullanıcı bu varlık bildirimi seçeneğiyle, istediği kullanıcıyla yazılı, sesli ve/veya görüntülü iletişime süratle başlayabilmelidir.

**2.6.21.58** Sistem, sunduğu birleşik mesajlaşma özelliğiyle, kurumun elektronik posta ve sesli posta altyapılarını konsolide etmesini sağlamalıdır. Kurumun yatırım yapmış olduğu Active Directory kimlik sisteminin üzerinde çalışarak, tek bir yönetim deneyimi ve sesli posta, elektronik posta ve faks üzerinde entegre güvenlik politikaları sağlamalıdır.

**2.6.21.59** Sistem, gelen yeni ya da güncel elektronik postaları, takvim öğelerini, iletişim kontaklarını ve görevleri, sunucu üzerine gelir gelmez mobil kullanıcılara iletmelidir.

**2.6.21.60** Eğer bir mobil cihaz kaybolursa ya da çalınırsa, kullanıcı sistemin web istemcisi üzerinden, mobil aygıtın içeriğini temizleyebilmeli ve aygıtın şifresini resetleyebilmelidir.

**2.6.21.61** Sistem yöneticileri, mobil aygıtlar için kullanıcı ya da aygıta özel, eklentiye (attachment) izin verme/vermeme, PIN geçerlilik süresi belirleme gibi politikalar belirleyebilmelidir.

**2.6.21.62** Mobil kullanıcı, sistemin mobil istemcisi üzerinden hem aygıtın içinde hem de sunucu üzerindeki posta kutusunda kapsamlı arama yapabilmelidir.

**2.6.21.63** Elektronik postaları izlemek için kullanılan bayraklar, mobil aygıtlar üzerinde de tamamen desteklenmelidir.

**2.6.21.64** Mobil aygıtlar, zengin HTML metnini desteklemelidir. Bir elektronik postaya mobil üzerinden cevap verildiğinde, postayı alan tüm kullanıcılar için HTML formatı korunmalıdır.

**2.6.21.65** Sisteme bağlı bir mobil kullanıcı uzun bir mesajı ya da eklentiyi tıkladığında, aygıt tüm mesajı tekrar yüklemeden gerekli bilgiyi getirebilmelidir.

**2.6.21.66** Mobil kullanıcılar, gelen toplantı taleplerini mobil aygıtlar üzerinden, PC deneyimiyle yanıtlayabilmeli, şirket dışında mesajlarını yine mobil aygıtları üzerinden yönetebilmelidir.

**2.6.21.67** Sistemin kurulumu için farklı sunucu rolleri olmalı, bu sunucu rolleri sayesinde kurulum için gereken zaman azaltılabilmeli, sistem yöneticisinin manual konfigürasyon için harcadığı zaman minimize edilebilmeli ve saldırıya açık olan yüzey alanını limitleyerek güvenlik artırılabilmelidir.

**2.6.21.68** Sistem, içinde hazır olarak bir En İyi Uygulamalar Analiz Aracı sunmalıdır. Bu araç konfigürasyonda servis kesintisine ya da güvenilirlik problemlerine yol açabilecek tutarsızlıkları tespit etmeli, yaygınlaştırma ve kurulumda yardım sağlamalıdır.

**2.6.21.69** PC istemcisi sisteme bağladığında, kullanıcı ağa log-in olduktan sonra, sistem kullanıcının profilini otomatik olarak konfigüre etmelidir.

**2.6.21.70** Sistemin, Microsoft Operations Manager 2005 and Systems Center Operations Manager 2007 gibi izleme ve yönetme araçları tarafından yönetilebilmesi ve izlenebilmesi için, kendisine özel tasarlamış yönetim paketlerine sahip olmalıdır.

**2.6.21.71** Sistem, posta kutularının taşınabilmesi için kapsamlı tek bir araca sahip olmalı, bu araç lokal veya global organizasyonlar arasındaki taşıma işlemlerini, karmaşıklığı düşürerek sağlayabilmelidir.

**2.6.21.72** Sistem, 3 seviye derinliğe inilebilen, navigasyonu kolaylaştıran grafik kullanıcı arayüzüne sahip bir yönetim konsolu sunmalıdır. Yönetim ve problem giderme araçları tek bir araç setinden çalıştırılabilmelidir.

**2.6.21.73** Sistem, komut satırı tabanlı bir yönetim katmanı da sağlamalıdır.

**2.6.21.74** Sistem 64-bit mimaride çalışmalıdır. Böylece sistem, sunucudaki posta kutusu ve kullanıcı sayıları arttığında, daha fazla belleğe erişip, yüksek performans ve güvenilirlik sağlayabilmelidir.

**2.6.21.75** Sistem Ipv6 desteğine sahip olmalıdır.

**2.6.21.76** Sistem Active Directory site yapısı üzerine inşa edilmiş bir routing topolojisine sahip olmalıdır.

**2.6.21.77** Sistem, yazılım geliştiricilerin posta kutusu ya da takvim bilgisini iş hattı sistemleri ya da diğer özel uygulamalar içine gömebileceği, genişletilebilir bir web servisi platformuna (API) sahip olmalıdır.

**2.6.21.78** Yazılımcılar sistemin web istemcisindeki işlevleri (elektronik posta, takvim vs.), yine sistemin sunduğu web bölümleri ile kendi portal uygulamalarına gömebilmelidirler.

**2.6.21.79** Sistem, DMZ üzerinde anti-spam filtrelemesi yapan bir role sahip olmalıdır.

**2.6.21.80** Sistem güvenliği, sağlayıcı şirket tarafından, daha iletiler sisteme gelmeden internet bulutu üzerinde e-posta, virüs, spam ve malware bloklaması yapan bir online servisle de desteklenebilmelidir.

**2.6.21.81** Sistem, kendi üzerinde de anti-virüs ve anti-spam yapan, dünyanın çeşitli şirketlerinden alınarak, çok yönlü kontrol yapabilen motorları içeren ek bir katman tarafından da korunabilmelidir.

**2.6.21.82** Sistemin veri tabanının bir kopyası ikinci bir disk setinde tutulabilmeli ve log shipping ile güncellenmesi sağlanabilmelidir. Böylece bir disk hatası ya da veri bozulması olayında, sistem yöneticisi süratle kopya veritabanına dönebilmeli ve ekonomik bir yolla daha yüksek çalışma zamanı elde edebilmelidir.

**2.6.21.83** Yüksek erişebilirlik bir aktif/pasif cluster yapısında sürekli replikasyon kullanılarak gerçekleştirilebilmelidir. Veri aktiften pasif sunucuya log shipping kullanılarak kopyalanabilmelidir. Bu yapıda paylaşılan depo yapısı (shared storage) gerekmemeli, böylece nodlar farklı coğrafyalarda bulunabilmelidir.

**2.6.21.84** Her sistem veritabanı, uzaktaki beklemedeki (standby) sunucusuna replike edilebilmeli, böylece tüm datacenter'ın çökmesi durumunda, kendini çabuk toparlayan bir elektronik posta ortamı sağlanabilmelidir.

**2.6.21.85** Sistem yama ve güncelleme yönetimi, sağlayıcı şirketin web sitesinden, sağlayıcı şirketin kurum içindeki güncelleme sunucusundan, ya da Microsoft Systems Management Server gibi yama ve güncelleme çözümlerinden otomatik olarak sağlanabilmelidir.

**2.6.21.86** Kurum içinde, varsayılan olarak gönderenin e-posta istemcisinden alıcının e-posta istemcisine gönderilen elektronik posta şifrelenmelidir.

**2.6.21.87** Transport Layer Security (TLS) destekleyen istemciler arasındaki bağlantı otomatik olarak şifrelenmelidir. Bu durumda sistem yöneticisinin herhangi bir aksiyon almasına gerek kalmamalıdır. Sistem, TLS'i içinde hazır gelen sertifikalarla otomatik olarak desteklemelidir.

**2.6.21.88** Sistem yöneticileri elektronik postalara, iletimdeyken, konusuna, içeriğine veya gönderen/alan adresine göre mesaj kategorizasyonu gerçekleştirmek için iletim kuralları (transport rules) uygulayabilmelidirler.

**2.6.21.89** Sistem, kurumların, kurumsal, kamusal ve legal ihtiyaçlarını karmaşık bir elektronik posta akış kontrolü ve politika motoru üzerinden yürütebilmelerini mümkün kılmalıdır.

**2.6.21.90** Sistem, kullanıcıların istemcileri üzerinde, önceden sistem yöneticileri tarafından tanımlanmış klasörlerde mesajlarını organize edebilmelerine izin vermelidir. Kurallara uygunluk gereksinimlerine göre otomatik bir süreç bu klasörleri tarayarak, klasördeki mesajların tutulması, geçerliliklerini yitirmeleri, günlüklerinin tutulması sağlanabilmelidir.

**2.6.21.91** Sistem yöneticileri elektronik postayı, veri tabanı, dağıtım listesi, kullanıcı ve kurum çapındaki kriterlere göre kayıt altına alabilmelidirler. Kayıt altına alma işlemi (Journaling), gönderen, alıcı ve mesaj içeriğine göre özelleştirilmelidir.

**2.6.21.92** Sistem yöneticileri legal bir araştırma gerektiğinde, kurumlarındaki tüm posta kutuları içinde hızlı full-text arama yapabilmelidir.

**2.6.21.93** E-posta sunucusu yazılımı istenen posta hesaplarını arşivleyebilmelidir.

**2.6.21.94** Her birim ve/veya birliğin kendine ait ve yalnızca kendi ayarlarını yönetebileceği e-posta sunucusu paneli olmalıdır.

### 2.6.22 E-Posta Sunucu Erişim Lisansı

**2.6.22.1** E-posta sunucusu Enterprise seviyede 300 adet erişim lisansı ile verilmelidir.

**2.6.22.2** E-posta sunucusu Standart seviyede 300 adet erişim lisansı ile verilmelidir.

### 2.6.23 Loglama ve Raporlama Ürünü

**2.6.23.1** Önerilen güvenlik duvarı sisteminin kayıt depolama ve takibini, raporlama işlemlerini gerçekleştirmek için aşağıda belirtilen şartlara uyan kayıt takip ve raporlama ürün/ürünleri alınacaktır.

**2.6.23.2** Aşağıda belirtilen özellikler yönetim ve kayıt sistemlerinin ayrı veya tek bir sistem olarak önerilecektir.

**2.6.23.2.1** Önerilen sistem, saniyede en az 25 GB/Gün veya 10.000 EPS/LPS log kayıt alabilmelidir.

**2.6.23.2.2** Log kayıt alanı olarak en az 10 TB depolama alanını desteklemelidir.

**2.6.23.2.3** Önerilen kayıt ve raporlama sistemi, güvenlik duvarı ile aynı marka olacaktır ve tam uyumlu bir şekilde entegre çalışabilecektir.

**2.6.23.2.4** Önerilen loglama ve raporlama ürünü appliance (kutu) ya da sanal sistem olarak teklif edilecektir. Sanal sistem teklif edilmesi durumunda kurumda kullanılan sanallaştırma sistemine uyumlu olacaktır.

**2.6.23.2.5** Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.

**2.6.23.2.6** 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.

**2.6.23.2.7** Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme veya raporlama özelliği olacaktır.

**2.6.23.2.8** Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilmelidir.

**2.6.23.2.9** Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.

**2.6.23.2.10** Merkezi yönetim dâhilinde bulunan bileşenlere ait anlık ortalama CPU, firewall, firewall cluster üzerinden akan tüm uygulamalar, kullanıcı IP adresleri ve dâhili kullanıcı isimleri gibi değerler anlık ve sürekli olarak görüntülenebilecektir.

**2.6.23.2.11** 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.

**2.6.23.2.12** Tutulan kayıt alanları baz alınarak özelleştirilmiş sorgular yazılabilmeli ve bu sorguların çıktıları, tablo, pie-chart şeklinde raporlar içerisine konulabilmelidir.

**2.6.23.2.13** PDF formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmelidir.

**2.6.23.2.14** Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp kayıtların yedekliliği sağlayabilmelidir.

**2.6.23.2.15** Yukarıda belirtilen seçeneklerden hangisi ile teklif edilirse edilsin, teklif edilen sistemlerin en az 5 yıl yazılım garantisi bulunmalıdır. 5 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

### 2.6.24 İzleme (Monitoring) Yazılımı

**2.6.24.1** İzleme yazılımı; sunucular, işletim sistemleri (Windows ve Linux/Unix), sanal platformlar, (“VmWare”), veri depolama üniteleri (farklı marka/modellerde “storage”) ve veritabanları, ağ anahtarları (“switch”) ve ağ yönlendiricileri (“router”) gerçek zamanlı olarak izlenebilmelidir.

**2.6.24.2** İzleme yazılımı; sunucuların ağ bağlantılarını, çalışan servisleri izleyebilmelidir.

**2.6.24.3** Sunucuların dizilim (“array”) yapılarını, yedeklilik (“raid”) yapılarını, sıcaklık ve fan değerleri, disk arızaları ve SEL loglarını izleyebilmelidir.

**2.6.24.4** İzleme yazılımı; Microsoft İşletim sisteminden detaylı bilgiler alabilmelidir.

**2.6.24.5** İzleme yazılımı; VMWare Host’ları izleyebilmelidir.

**2.6.24.6** İzleme yazılımı; Ağ cihazlarını izleyebilmelidir.

**2.6.24.7** İzleme yazılımı; Ağ cihazlarını harita üzerinde gösterebilmelidir.

**2.6.24.8** İzleme yazılımı; Ağ cihazlarından Netflow ve Sflow ile 100 cihaz ve 5000 Adet sensörden kayıt alabilmelidir.

**2.6.24.9** İzleme yazılımı; Mysql, Mssql ve Oracle Veri Tabanlarını izleyebilmelidir.

**2.6.24.10** İzleme yazılımı; sistem bileşenlerinde oluşabilecek sistemsel kırılganlıkların ya da hataların e-posta ve/veya kısa mesaj ile aktif bildirimini yapabilecek otomatik ve kişiselleştirilebilir özellikte bir uyarı/alarm sistemine olanak tanımalıdır.

**2.6.24.11** Ürün; 5 yıllık lisansları birlikte verilecektir.

### 2.6.25 Çok Faktörlü Kimlik Doğrulama Yazılımı

**2.6.25.1** Teklif edilen ürün 1000 adet anlık local veya uzak kullanıcı desteğine sahip olmalıdır.

**2.6.25.2** Teklif edilen ürün 500 adet kullanıcı sertifika desteğine sahip olmalıdır.

**2.6.25.3** Teklif edilen ürün en az 10 adet kullanıcı grubu oluşturma desteğine sahip olmalıdır.

**2.6.25.4** Teklif edilecek ürün donanım olarak veya sanal olarak VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0 / 5.5 / 6.0 / 7.0 / 8.0, Microsoft Hyper-V Server ortamlarında çalışabilmelidir.

**2.6.25.5** Teklif edilen ürün tek olarak lisanslanmalı ve gerektiğinde yedekli Active-Passive HA desteğine sahip olmalıdır.

**2.6.25.6** Teklif edilecek ürün SSO (single sign on) desteği olmalıdır ve aşağıdaki kaynaklardan beslenebilmelidir.

- **2.6.25.6.1** AD (Active directory) sorgulama (AD polling) veya AD agent iletişimi
- **2.6.25.6.2** Kerberos
- **2.6.25.6.3** REST API
- **2.6.25.6.4** Radius Accounting
- **2.6.25.6.5** SSO Login Portal
- **2.6.25.6.6** Syslog

**2.6.25.7** Teklif edilen ürün sertifika yönetimi yapabilmelidir.

**2.6.25.8** Teklif edilecek ürün, kullanıcı sertifika yönetimini “VPN” ve “Windows Desktop Authentication” bağlantılar için oluşturup doğrulayabilmelidir.

**2.6.25.9** Teklif edilen ürün Radius Accounting Proxy desteği olmalıdır.

**2.6.25.10** Teklif edilen ürün harici AD, LDAP, Radius desteği olmalıdır.

**2.6.25.11** Teklif edilen ürün Radius ürün olarak kullanılabilmelidir.

**2.6.25.12** Teklif edilen ürün HTTPS üzerinden yönetilebilmelidir.

**2.6.25.13** Teklif edilen ürün kullanıcı girişlerini kayıt altına alabilmeli ve harici loglama sistemlerine aktarabilmelidir.

**2.6.25.14** Teklif edilen ürün CPU ve memory kullanımlarını, kullanıcı adet istatistiklerini önyüz üzerinden gösterebilmelidir.

**2.6.25.15** Teklif edilen ürün SNMP v1/v2c ve v3 desteği olmalıdır. MIB bilgileri üzerinden soğulama yapılabilmelidir.

**2.6.25.16** Teklif edilen ürün admin kullanıcılarına yetkilendirme yapılabilmelidir.

**2.6.25.17** Teklif edilen ürün log kayıtları HTTPS arayüz üzerinden filtrelenebilir şekilde sorgulanabilmelidir.

**2.6.25.18** Teklif edilen ürün log kayıtlarını harici syslog server'lara gönderebilmelidir.

**2.6.25.19** Teklif edilen ürün 5 (beş) yıllık yazılım destek paketi ile verilmelidir.

### 2.6.26 Web Zafiyet Tarama Yazılımı

**2.6.26.1** Teklif edilen sistem, web tabanlı yönetim arayüzüne sahip olacak ve web arayüzüne erişim parola korumalı olacaktır.

**2.6.26.2** Teklif edilen ürün lisansı, aynı ağ üzerinde sınırsız IP adresini tarayabilecek kapasitede olmalıdır.

**2.6.26.3** Ürün içerisinde kullanıcı tarafından özelleştirilebilecek en az 15 adet tarama şablonu (template)

**2.6.26.4** Ürün üzerinde en az HTML, CSV ve PDF formatlarında rapor çıktısı alınabilmelidir.

**2.6.26.5** Ürün üzerinde oluşturulacak olan taramaların zamanlanması (schedule) mümkün olmalıdır.

**2.6.26.6** Ürün tarama sonucunda zafiyet, uyumluluk, iyileştirme ve tarihsel çıktıları görüntülemeye imkân sağlayacak veriler yer almalıdır.

**2.6.26.7** Ürün yapılan taramaların sonucunda e-posta ile bilgilendirme yapabilmelidir

**2.6.26.8** Ürün tamamlanan 2 (iki) zafiyet tarama arasındaki farkları (diff) gösterebilmelidir.

**2.6.26.9** Ürün tarama sonucu oluşan bulguları CVSS formatında 5 (beş) ana grupta (Critical, High, Medium, Low, Info) gösterebilmelidir

**2.6.26.10** Ürün CIS, DISA STIGs, PCI standartlarına uygun yapılandırma kontrolü yapabilmelidir.

**2.6.26.11** Ürünün Ipv4 ve Ipv6 desteği olmalıdır

**2.6.26.12** Ürüne ait tüm bileşenler (component) web arabirimden otomatik olarak güncellenebilmelidir.

**2.6.26.13** Ürünün tüm fonksiyonları yerel ve internet erişimi olmayan ağlarda çalışmalıdır. Bulut (cloud) bağımlılığı olmamalıdır. Güncellemeler elle de yapılabilmelidir.

**2.6.26.14** Ürün yetkili hesap üzerinden zafiyet taramaları yapabilmeli ve en az aşağıdaki belirtilen kimlik doğrulama yöntemlerini kullanabilmelidir;

**2.6.26.14.1** Windows: Kerberos, LM Hash, Password, NTLM Hash

**2.6.26.14.2** HTTP: Http Login Form, Basic/Digest Authentication, Automatic Authentication, HTTP cookies

**2.6.26.15** Ürün aşağıda belirtilen türdeki varlıklar üzerinde, belirtilen kontrolleri gerçekleştirebilmelidir;

**2.6.26.15.1** Güvenlik duvarı, router, yazıcı, veri depolama vb. gibi ağ cihazlarının web arayüzleri

**2.6.26.15.2** Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries işletim sistemleri

**2.6.26.15.3** Oracle, SQL Server, MySQL, PostgreSQL veritabanı sistemleri

**2.6.26.15.4** Microsoft Azure, Amazon Web Service, Salesforce ve Rackspace gibi bulut altyapısı üzerinden host edilen web arayüzleri

**2.6.26.15.5** Kurumların mevzuatları uyumluluğu açısından tarama gereksinimlerinin karşılaması

**2.6.26.15.6** PCI DSS gereksinimlerine göre yapılandırma kontrolü

**2.6.26.16** 2.6.26.16 Teklif edilen ürün 20 adet domaini sınırsız sayıda tarayabilecek şekilde lisanslanacaktır."

### 2.6.27 Ayrıcalıklı Erişim Yönetimi (PAM) Ürünü

**2.6.27.1** PAM çözümü VMvare/HyperV/KVM sanallaştırma platformlarında çalışabilmelidir.

**2.6.27.2** PAM çözümü en az 30 kullanıcı kullanımı için teklif edilmelidir. Şartname de belirtilen sistemin çalışması için gerekli tüm lisanslar 5 Yıl süre ile teklife ilave edilmelidir.

**2.6.27.3** Kurulum için herhangi bir ilave işletim sistemi lisansına gerek olmamalıdır. Ürün kendi işletim sistemi ile verilmelidir.

**2.6.27.4** Ayrıcalıklı hesapların şifre güvenliğini sağlamalıdır.

**2.6.27.5** Ayrıcalıklı hesapların şifre ve erişim bilgilerini kendi üzerinde güvenli bir şekilde muhafaza edebilmelidir.

**2.6.27.6** Farklı kullanıcı tipleri (çalışanlar/danışmanlar/farklı departman kullanıcıları vs.) için farklı PAM erişim arayüzleri oluşturarak kullanıcılara atanan sadece ilgili IP aralığından erişim sağlanabilmelidir.

**2.6.27.7** Bir Folder/Kasa' nın admin kullanıcısı diğer folder/kasa'ların içerisini görememeli ve erişim bilgilerine ulaşamamalıdır.

**2.6.27.8** Ayrıcalıklı kullanıcıların ayrıcalıklı sistemlere erişimlerini video kayıtları ile saklayabilmelidir

**2.6.27.9** Aktif olan kullanıcıları monitör edebilmeli ve bağlantılarını sonlandırabilmelidir.

**2.6.27.10** Aktif uzak masaüstü bağlantılarını canlı olarak izleyebilmeli ve sonlandırabilmelidir.

**2.6.27.11** Kaydedilmiş video içerisinde filtreleme yapabilmelidir.

**2.6.27.12** Sunucu, Firewall, Network cihazı gibi kritik sistemlere erişen ayrıcalıklı kullanıcıların erişecekleri kritik sistemlerin şifre ve erişim bilgilerini bilmeye gerek kalmadan erişimlerini sağlayabilmeli ve kullanıcının tüm hareketlerini kayıt altına alabilmelidir.

**2.6.27.13** Kritik sistemlerin (Sunucu, Firewall, Network cihazı vs.) şifre güvenliğini sağlamak adına şifreleri otomatik olarak belli periyotlarda ve giriş/çıkış işlemlerinden sonra değiştirebilmelidir.

**2.6.27.14** Bağlantı yapmadan önce şifre doğrulama yapabilmelidir.

**2.6.27.15** Şifre değişikliği geçmişini gösterebilmelidir.

**2.6.27.16** Check-in / Check-out özelliği ile kritik sisteme aynı anda birden fazla kullanıcının bağlanmasını engelleyebilmelidir.

**2.6.27.17** Kritik sistemlere erişirken yetkili yöneticiden onay isteme mekanizmasına sahip olmalıdır ve bunu en az 3 aşamaya kadar uygulayabilmelidir.

**2.6.27.18** Onay mekanizmasını bir yönetici grubundan yetki istenecek şekilde de tanımlayabilmeli ve bu grup içinden en az 2- 3 kullanıcının onaylaması ile erişimin aktif edileceği şekilde ayarlanabilmelidir.

**2.6.27.19** ZTNA kabiliyetlerine sahip olmalıdır ve Sıfır güven prensiplerine göre tasarlanmış bir yapıya native olarak entegre olabilmelidir.

**2.6.27.20** SSH/Uzak masa üstü gib erişimleri web browser üzerinden veya uygulama kullanarak yapabilmelidir.

**2.6.27.21** SSH ile komut satırından erişimlerde istenmeyen ve riskli görülen komutların çalıştırılmasını engelleyebilmelidir.

**2.6.27.22** İstenmeyen bir komut kullanıldığında engelleyebildiği gibi alarm olarak da bildirmelidir ve log kayıtlarını almalıdır.

**2.6.27.23** AD/LDAP, RADIUS, SAML yöntemleri ile entegre olabilmeli ve kullanıcı doğrulama yapabilmelidir.

**2.6.27.24** Kullanıcılara istenilen yetki seviyelerinde (standart/admin vs.) roller tanımlanabilmelidir.

**2.6.27.25** Bir hedef sistem üzerinde script vs çalıştırmak için job'lar oluşturabilmelidir ve onay mekanizması burada da desteklenmelidir.

**2.6.27.26** Unix/Linux gibi sistemlere şifre haricinde private key kullanarak da erişim sağlayabilmelidir.

**2.6.27.27** Gerektiğinde kullanılacak secret'lar dışarıda oluşturulup içeriye import edilebilmelidir.

**2.6.27.28** SSH erişimlerinde TOTP kullanılabilmelidir.

**2.6.27.29** Kullanıcı erişimlerinde 2FA kullanmak için üreticiye ait tokenlar kullanılabilmelidir.

**2.6.27.30** Kullanıcılar PAM arayüzüne bağlandıktan sonra kendi personel folder'ları içinde kişisel ve lokal şifrelerini muhafaza edebilmelidirler.

**2.6.27.31** Ürünle gelen Launcher'lar haricinde de araçlar oluşturulabilmelidir.

**2.6.27.32** Kullanıcı erişimlerinde source IP kısıtlaması yapılabilmelidir.

**2.6.27.33** Kullanıcı erişimlerinde, bağlanacak kullanıcının sadece belli bir zaman diliminde gelebilmeleri ayarlanabilmelidir.

**2.6.27.34** Web arayüzün'den erişimler yapabilmelidir ve şifre girişleri PAM tarafından otomatik olarak girilebilmelidir.

**2.6.27.35** Windows, Linux, MacOS işletim sistemleri desteklenmelidir.

**2.6.27.36** Rest API desteğine sahip olmalıdır.

**2.6.27.37** Log toplayabilmeli ve raporlama yapabilmelidir.

**2.6.27.38** Otomatik olarak yedekleme yapılabilmelidir.

**2.6.27.39** Süreklilik için Aktif/Pasif veya Aktif/Aktif olarak yedekli çalışabilmelidir.

## 2.7 VERİ MERKEZİ OPERASYON HİZMETİ

### 2.7.1 Hizmetin Konusu ve Detaylar

**2.7.1.1** İDARE Veri Merkezi ve Yedek Veri Merkezi altyapısının ve bakımının 5 yıl süre ile sağlanması işidir.

### 2.7.2 İşin Kapsamı ve Detaylar

**2.7.2.1** Veri Merkezi ve Yedek Veri Merkezi mimari tasarımı yapılacaktır.

**2.7.2.2** Veri Merkezi Barındırma Hizmeti verilecektir.

**2.7.2.3** Yedek Veri Merkezi Barındırma Hizmeti verilecektir.

**2.7.2.4** Veri Merkezi ve Yedek Veri Merkezi Erişim Hizmetleri verilecektir.

**2.7.2.5** Veri Merkezi ve Yedek Veri Merkezi kurulum hizmetleri verilecektir.

**2.7.2.6** Veri Merkezi ve Yedek Veri Merkezi 7/24 bakım ve destek hizmeti verilecektir.

### 2.7.3 Genel Hükümler ve Detaylar

**2.7.3.1** Ana veri merkezi en az TIER 3 standardında olmalıdır.

**2.7.3.2** Veri Merkezi internet hızı, MPLS hızları, veri merkezleri arası bağlantı hızı değerlerini kurum isterse arttırabilir veya düşürebilir.

**2.7.3.3** Bu şartnamede belirtilen işlerin, şartnamede tarif edildiği şekilde ve anahtar teslimi olarak tamamlanması esastır.

**2.7.3.4** Veri merkezi altyapısı işe başlama tarihinden itibaren en geç 30 takvim gününde sağlanacaktır.

**2.7.3.5** Veri Merkezi hizmetleri için hızlar ve adetler artırılabilir. Firma ihalede yüksek hızlar için de fiyat listesini iletecektir.

**2.7.3.6** Her 12 aylık dönem sonunda Veri merkezi ile ilgili hizmetlerin fiyatları Tüfe ve Üfe artış oranının ortalaması kadar artırılacaktır.

**2.7.3.7** Talep edilen lokasyonlar için erişim altyapısı, işe başlama tarihinden itibaren en geç 30 takvim günü içinde sağlanacaktır. Ancak, kablolama veya altyapıda değişiklik talep edilmesi sonucu operasyonel süreçte oluşacak olan YÜKLENİCİ bağımsız durumlarda bu süre gözden geçirilebilir. Bu lokasyonlar dışındaki erişim talepleri, standart SLA süreleri doğrultusunda kurulacaktır.

**2.7.3.8** İDARE'den kaynaklanacak gecikmeler yukarıdaki süreye eklenecektir.

**2.7.3.9** YÜKLENİCİ, teklif edilen ihale bedelleri dışında fiyat farkı talep etmeyecektir. İşin kapsamının değişmesi durumunda idari şartnamenin ilgili koşulları uygulanacaktır.

**2.7.3.10** İDARE bu şartnamede bahsedilen hizmetlerden istediğini alabilir, istediğinin sayısını artırabilir veya eksiltebilir. YÜKLENİCİ sadece verilen hizmetleri aylık faturalandıracaktır.

**2.7.3.11** Kabin Barındırma, Veri Merkezi Internet (Aktif ve Pasif DC), DDoS Atak Önleme Hizmeti, Noktadan Noktaya Metro Ethernet ve MPLS VPN Metro Ethernet hizmetleri YÜKLENİCİ tarafından verilecektir.

### 2.7.4 Proje Yönetimi ve Proje Planı Detaylar

**2.7.4.1** Sözleşmenin imzalanmasını takiben 10 gün içerisinde yüklenici proje planını İDARE'nin onayına sunacaktır.

**2.7.4.2** İDARE, YÜKLENİCİ tarafından sunulan planı 5 gün içerisinde onaylayacaktır veya düzeltilmesi için geribildirimde bulunacaktır.

**2.7.4.3** YÜKLENİCİ ihale kapsamında sağlanacak altyapıların kurulumu için bir proje yöneticisi görevlendirecektir.

### 2.7.5 Proje Başlıkları ve Detaylar

**2.7.5.1** İDARE tarafından öngörülen proje aşamaları aşağıdadır. Firma proje aşamalarını, veri merkezi altyapısını ve ürünleri teklifinde detaylandıracaktı.

**2.7.5.2** Veri Merkezi ve Felaket Kurtarma veri merkezi Ağ altyapısı mimarisi, bu şartname başlıklarına uygun bir şekilde firma tarafından hazırlanıp İDARE onayına sunulacaktır.

**2.7.5.3** Yeni Veri Merkezi, Felaket Kurtarma veri merkezi, Bölgeler, bağlantıları ve yedekliliği bu şartname başlıklarına uygun bir şekilde firma tarafından hazırlanıp İDARE onayına sunulacaktır

**2.7.5.4** Veri Merkezi ve Yedek Veri Merkezine kurulacak ürünler İDARE tarafından sağlanacaktır.

### 2.7.6 Yüklenici, Lokasyon ve Bina Detaylar

**2.7.6.1** YÜKLENİCİ veya HİZMET ALDIĞI VERİ MERKEZİ en az 2 şehirde veri merkezi hizmeti yönetimi tecrübesine sahip olmalıdır.

**2.7.6.2** Yüklenicinin Ana Veri Merkezi en az Tier III sertifikasına sahip olmalıdır.

**2.7.6.3** TUV Energy Efficient Data Center, ISO 27001-Bilgi Güvenliği sertifikası, ISO 22301- İş sürekliliği sertifikası, PCI DSS- Payment Card Industry Data Security Standard, ISO 20000 – IT Servis yönetimi sertifikası ve ISO 22320 – Emergency Management sertifikasına sahip olmalıdır.

**2.7.6.4** YÜKLENİCİ veya HİZMET ALDIĞI VERİ MERKEZİ en az 3000 m2 beyaz alan üzerinde veri merkezi hizmeti yönetimi tecrübesine sahip olmalıdır.

**2.7.6.5** YÜKLENİCİ, İDARE'ye 2 veri merkezi üzerinden hizmet sunabilecektir.

**2.7.6.6** Veri Merkezilerinden bir tanesi İstanbul Büyükşehir Belediyesi il sınırları içerisinde olmalıdır.

**2.7.6.7** Veri Merkezleri en az 700 kg/m2 taşıma kapasitesine sahip olmalıdır.

**2.7.6.8** İkincil veri merkezi birinci veri merkezinden en az 350 km mesafede olmalıdır.

**2.7.6.9** Veri Merkezlerinin her ikisinin de Deprem Yönetmeliğine uygun sağlamlaştırma çalışmalarının yapılmış olması, YÜKLENİCİ'nin yapılan çalışmaları belgelendirmesi ve her iki veri merkezi için Deprem Yönetmeliğine uygunluk belgesinin İdareye sunulması gerekmektedir.

### 2.7.7 Network Erişim Hizmeti ve Detaylar

**2.7.7.1** Erişim hizmeti YÜKLENİCİ veya HİZMET ALDIĞI VERİ MERKEZİ'nin POP (Point of presence) noktası üzerinden sağlanmalıdır.

**2.7.7.2** Erişim hizmeti asgari 2 farklı fiber optik güzergâhtan sağlanmalıdır.

**2.7.7.3** YÜKLENİCİ veya HİZMET ALDIĞI VERİ MERKEZİ 'nin en az 2 Tier-1 ISP ile IP arabağlantısı olmalıdır.

### 2.7.8 Enerji Altyapısı ve Detaylar

**2.7.8.1** Veri merkezi tesislerinin enerji alt yapı işletmeni sorumlusu alanında en az 5 yıllık iş tecrübesine sahip elektrik mühendisi veya elektrik- elektronik mühendisi olmalıdır.

**2.7.8.2** Veri merkezi orta gerilim enerjisi iki farklı orta gerilim hücresinden sağlanacak ve asgari 2N yapıda olmalıdır. u5.8.3. Veri merkezi, iki farklı transformatör'den beslenecek, asgari 2N yapıda olmalıdır.

**2.7.8.3** Veri merkezini besleyen jeneratörler asgari N+1 yedekliliğe sahip olmalıdır.

**2.7.8.4** Veri merkezini besleyen jeneratör tankları, veri merkezi standby yükünde veri merkezini en az 24 saat besleyecek kapasiteye sahip olmalıdır.

**2.7.8.5** Veri merkezi içerisindeki yükler asgari 2 farklı UPS grubu tarafından beslenmelidir. UPS grupları kendi içerisinde minimum N+1 yedekli olmalıdır.

**2.7.8.6** UPS grupları kendi içerisinde senkron çalışmalıdır.

**2.7.8.7** UPS'ler farklı odalarda olacak ve bu odaların iklimlendirmesi asgari N+1 soğutma sistemi ile sağlanacaktır.

**2.7.8.8** Her UPS grubu, tam yükte asgari 15 dk. Back-up sağlayabilecek akü gruplarına sahip olacaktır.

**2.7.8.9** Her kabinette asgari 2 adet PDU olmalı ve her PDU farklı UPS grupları tarafından beslenmelidir.

**2.7.8.10** Kabinetlerde bulunan PDU'lar (metered) uzaktan enerji tüketimi izlenebilecek şekilde olmalıdır.

**2.7.8.11** Her kabinde port bazlı ölçüm yapan PDU' lar bulunuyor. Buradan da tüketilen enerji bedeli EMM ile entegre şekilde otomatik faturalamaya yansımaktadır. Enerji tüketimi izlenip, fatura üretim sistemine veri aktarılmakta ancak bununla ilgili müşteri tarafında bir arayüz sağlanamamaktadır.

**2.7.8.12** Sistemin topraklama ölçümlerinin her yıl yapılmalı ve EMO'nun (Elektrik Mühendisleri Odası) belirttiği değerlerde olmalıdır.

**2.7.8.13** Enerji ve veri kablolaması veri merkezi içerisinde birbirinden ayrı rotalardan giderek kabinlerde sonlandırılmalıdır.

### 2.7.9 İklimlendirme ve Detaylar

**2.7.9.1** İklimlendirme sistemi asgari N+1 yedekli olmalıdır.

**2.7.9.2** Kullanılan klima sistemi hassas kontrollü olmalıdır.

**2.7.9.3** İklimlendirme altyapısı optimum verimlilik için tasarlanmış olmalıdır. (Sıcak hava ya da soğuk havanın izolasyonu).

**2.7.9.4** İklimlendirme sistemi en az 1,25 kw/m2 soğutma kapasitesine sahip olmalıdır.

**2.7.9.5** Veri merkezlerinin bulunduğu konumların iklim koşullarında ve enerji verimliliğine göre uygun klima sistemleri olmalı ve işletme maliyetleri açısından PUE değeri ortalama (Yaz Kış) ortalama 1.5'i geçmemelidir.

**2.7.9.6** Veri merkezlerinden en az bir tanesi serbest soğutma (free cooling) ile iklimlendirme ihtiyaçlarını karşılayabiliyor olmalıdır.

### 2.7.10 Fiziksel Güvenlik ve Detaylar

**2.7.10.1** Kampüs Güvenliği

**2.7.10.1.1** Kampüs çevresinde, kampüste veri merkezi bulunduğuna dair tabela, afiş gibi bilgilendirme sistemleri bulunmamalıdır.

**2.7.10.1.2** Kampüsü çevreleyen yeterince yüksek, üzerinde dikenli tel bulunan beton duvarlar bulunmalıdır.

**2.7.10.1.3** Kampüsü çevreleyen duvarlar üzerinde gece ve gündüz görüş kamera sistemi bulunmalıdır. Kameralar 7x24 kayıt yeteneğine sahip olmalı ve kamera kayıtları asgari 1 ay süre ile saklanmaktadır.

**2.7.10.1.4** Kampüs girişinde, kampüse giren kişiler ve araçlar için bir güvenlik bulunmalıdır.

**2.7.10.1.5** Kampüs girişinde yolu loglayan Plaka tanıma sistemi olmalıdır. Bu kayıtlar asgari 1 ay süre ile saklanmalıdır.

**2.7.10.1.6** Kampüse girişte bariyer sistemi bulunmalı, girişte 7x24 güvenlik sorgulaması yapılmalıdır.

**2.7.10.1.7** Kampüse giren yabancı araçlar için bagaj kontrolü yapılmalıdır.

**2.7.10.2** Veri Merkezi Bina Güvenliği

**2.7.10.2.1** Veri merkezi binasına girişte manyetik kartlı geçiş sistemi bulunmalıdır.

**2.7.10.2.2** Ziyaretçiler binaya X ray cihazından geçerek girebilmelidir.

**2.7.10.2.3** Ziyaretçiler bina girişinde Ziyaretçi kayıt sistemine kaydedilmelidir.

**2.7.10.2.4** Ziyaretçilere ziyaretleri boyunca kullanacakları bir kart sağlanmalı ve kartlar sadece ziyarete uygun alanlara, tanımlı süreler içerisinde giriş için yetkilendirilmelidir.

**2.7.10.2.5** Ziyaretçiler, ziyaretleri boyunca kartları görünür bir yere asmaları konusunda bilgilendirilmelidir.

**2.7.10.3** Veri Merkezi Beyaz Alan Güvenliği

**2.7.10.3.1** Beyaz alan girişinde bina girişindeki manyetik karta ek biyometrik (örneğin retina tarama) bir güvenlik sistemi olmalıdır.

**2.7.10.3.2** Beyaz alan girişinde aynı anda bir kişinin girişine imkân tanıyacak bir sistem kurulmalıdır.

**2.7.10.3.3** Beyaz alana tüm giriş ve çıkış kayıtları tutulmalıdır ve asgari 1 yıl süre ile saklanmalıdır.

**2.7.10.3.4** Beyaz alan içerisinde ziyaretçilere yapacakları çalışma süresince eşlik ediliyor olmalıdır.

**2.7.10.3.5** Beyaz alan giriş çıkış noktaları kameralar ile izlenmeli; Kamera görüntüleri en az 1 ay geriye yönelik saklanmalıdır. İDARE'nin talebi sonrasında ilgili kayıtlar İDARE'ye denetim amacıyla yerinde gösterilebilir.

**2.7.10.3.6** Beyaz alana malzeme girişleri ayrı bir kapıdan yapılmalı tüm giriş kapıları 6 saat yangına dayanıklı kapı özelliğinde olmalıdır.

**2.7.10.4** Veri Merkezi Kabin Güvenliği için YÜKLENİCİ, İDARE'nin talep etmesi halinde İDARE'ye sağlanacak kabinler için kart okuyucu ve parmak izi okuyucu konumlandıracaktır.

### 2.7.11 Yangın, Yangın Algılama ve Detaylar

**2.7.11.1** Veri merkezi ve kampüs çevresinde patlama ve yanma riski yüksek bir tesis bulunmamalıdır.

**2.7.11.2** Veri merkezi binası için yangın algılama ve söndürme sistemi bulunmalıdır.

**2.7.11.3** Veri merkezi beyaz alanı için sistemlere ve personele zarar vermeyecek yapıda uluslararası standartlara uygun yangın algılama ve söndürme sistemi bulunmalıdır.

**2.7.11.4** Acil çıkış kapısı/kapıları olmalıdır. Gerekli ışıklandırma ve yönlendirmeler içeride yapılmış olmalıdır.

**2.7.11.5** Veri merkezinin bulunduğu bina ve beyaz alanlar için atanmış yangın sorumluları/sorumlulukları bulunmalıdır.

**2.7.11.6** Veri merkezi bina ve kampüs için yangın tahliye planı bulunmalıdır.

**2.7.11.7** Veri merkezlerinden en az birinde 120 dakika yangına dayanıklı duvarlar olmalıdır.

### 2.7.12 Su ve Sel Baskını Önlemleri ve Detaylar

**2.7.12.1** Veri merkezi beyaz alanın bulunduğu binanın sel baskınına karşı koruması için kampüs çevresinde engel bulunmalıdır.

**2.7.12.2** Veri merkezi beyaz alanının bulunduğu binada herhangi bir noktadan su sızıntısı, damlama ve akıntı (çatı dahil) olmamalıdır.

**2.7.12.3** Veri merkezi beyaz alanın üzerinde ıslak zemin bulunmamalıdır.

### 2.7.13 Diğer Önlemler ve Detaylar

**2.7.13.1** Binada haşere ve farelere karşı önlem alınmalıdır ve düzenli olarak ilaçlanmalıdır.

**2.7.13.2** Veri merkezi için yıldırım tehlikesine karşı önlemler alınmış olmalıdır.

**2.7.13.3** YÜKLENİCİ, İDARE'nin talep etmesi halinde veri merkezi içerisinde kullanılan ekipmanlar için periyodik kontrol ve bakımlarının formlarını yerinde gösterecektir.

### 2.7.14 Veri Merkezi Beyaz Alan Özellikleri ve Detaylar

**2.7.14.1** Veri merkezi beyaz alan içerisinde sıcak ve soğuk hava koridoru uygulaması yapılacaktır.

**2.7.14.2** Yükseltilmiş döşeme yüksekliği asgari 45 cm olmalıdır.

**2.7.14.3** Yükseltilmiş döşeme – tavan (/varsa alçaltılmış tavan) arası asgari 3 metre olmalıdır.

**2.7.14.4** Yükseltilmiş döşeme altı, epoksi ile kaplanmış olacaktır.

**2.7.14.5** Enerji ve veri kablolamasının döşeme altında yapmış olması durumunda, havalandırmayı engellemeyecek bir yapı oluşturmuş olmalıdır.

**2.7.14.6** Veri merkezi beyaz alan nem değeri %20-%80 RH arasında tutulmalıdır.

**2.7.14.7** Veri merkezi beyaz alan, soğuk hava koridoru ısı değeri ortalaması 18-27 derece arasında olmalıdır.

### 2.7.15 Ofis Alanı ve Detaylar

**2.7.15.1** Veri merkezi ile aynı kampüs içerisinde paylaşımlı çalışma alanı sağlanmaktadır. Bu paylaşımlı çalışma alanında mobilya, internet, enerji ve standartlara uygun çalışma koşulları sağlanmaktadır. Bilgi güvenliği sebebi ile Beyaz Alan ile ofis alanı arası kablolama yapılmamaktadır

**2.7.15.2** Veri merkezi ile aynı kampüs içerisinde 2 kişilik kapalı ofis alanı sağlanacaktır.

**2.7.15.3** Ofis alanı ile mobilya ve yerel alan ağı da sağlanacaktır.

**2.7.15.4** Ofis alanına giriş bina girişinde kullanılan kartlar ile sağlanacaktır.

**2.7.15.5** Ofis kapısında kullanılan kart okuyucu merkezi güvenlik sistemi ile entegre olup merkezi olarak yetkilendirme ve raporlamalar gerçekleştirilebilecektir.

**2.7.15.6** Ofis alanı içerisinde her bir masada 2xenerji ve 1xbakır network kablolama yapılmış olacaktır.

## 2.7.16 Veri Merkezi Hizmetleri ve Detaylar

**2.7.16.1** Yerinde Destek

**2.7.16.1.1** Veri merkezinde 7/24 tüm resmi ve dini bayramlar da dahil olmak üzere kesintisiz olarak hizmet verilecektir.

**2.7.16.1.2** Veri merkezi yerinde destek kapsamında sunucuların veya cihazların uzaktan açılıp kapanması, gerekli fiziksel kontrol ve müdahalelerinin yapılması hizmetleri verilecektir.

**2.7.16.2** İzleme Hizmetleri

**2.7.16.2.1** Ortam sıcaklık değeri izlenmeli, raporlanabilmeli, değer aşımları için alarm mekanizması bulunmalıdır.

**2.7.16.2.2** Ortam nem değeri izlenmeli, raporlanabilmeli, değer aşımları için alarm mekanizması bulunmalıdır.

**2.7.16.2.3** Jeneratörlere ait yakıt depoları seviyesi standart süreç ya da otomasyon ile izlenmelidir.

**2.7.16.2.4** Veri merkezi beyaz alan için minimum 6 saatte bir fiziksel ve görsel kontrol süreci bulunmalıdır.

**2.7.16.2.5** Veri merkezinde veri merkezi operasyon ekibi 7x24 zaman diliminde asgari her 6 saatte bir genel kontrol gerçekleştirecektir.

**2.7.16.2.6** Veri merkezinde Enerji ve iklimlendirme ekibi 7x24 zaman diliminde asgari her 6 saatte bir genel kontrol gerçekleştirecektir.

**2.7.16.2.7** Veri merkezinde güvenlik ekibi 7x24 zaman diliminde asgari her 6 saatte bir genel kontrol gerçekleştirecektir.

**2.7.16.2.8** Veri merkezi içerisinde PDU'ya kadar tüm enerji tüketimlerini ve IT Ekipmanları ve Servisleri dâhil tüm sistemlerin ayakta çalışır halde bulunduğunu izleyecek BMS ve DCIM sistemleri bulunmalıdır.

**2.7.16.3** Önleyici Bakım Hizmetleri

**2.7.16.3.1** Tüm ekipmanların (Trafo, Jeneratör, UPS, Klima-İç ve Dış Üniteler, Elektrik Panoları, Yangın Algılama ve Söndürme Sistemleri, Geçiş Kontrol Sistemleri, Kapalı Devre TV Sistemleri, …vb) bakım anlaşmalarını yapmış olmalıdır.

**2.7.16.3.2** Tüm enerji ve altyapı ekipmanları kontrolü için veri merkezinde 7/24 personel bulundurulmalı ve 6 saatte bir kontrol yapılmalıdır.

## 2.7.17 Erişim Hizmetleri ve Detaylar

**2.7.17.1** Erişim Altyapısı

**2.7.17.1.1** YÜKLENİCİ tarafından İDARE talebi doğrultusunda Veri Merkezi Internet, Veri Merkezi MPLS VPN, Noktadan Noktaya Bağlantı hizmetlerinden herhangi biri veya tümünü İDARENİN kullanımına sunulacaktır.

**2.7.17.2** Metro Ethernet İnternet Hizmeti

**2.7.17.2.1** Yüklenici, sağladığı Metro Ethernet internet hizmeti için en fazla 5 dakikalık aralıklarla, günlük, haftalık, aylık ve yıllık olarak trafik miktarlarının izlenebileceği web ara yüzü (MRTG) sunacaktır.

**2.7.17.2.2** Merkez Veri Merkezi için teklif edilecek metro ethernet internet hizmeti için Erişim Hızı 200 Mbit/s olacaktır.

**2.7.17.2.3** Yedek Lokasyon Veri Merkezi için teklif edilecek metro ethernet internet hizmeti için Erişim Hızı 50 Mbit/s olacaktır.

**2.7.17.2.4** Teklif edilecek Metro Ethernet hizmet altyapısı en az 1000 Mbit/s hızı destekleyecek kapasitede olacaktır.

**2.7.17.2.5** Müşterinin kendi alacağı IP adres blokları Metro Ethernet hizmeti üzerinde kullanılabilecektir.

**2.7.17.2.6** IP adres bloklarının değişmesi durumunda yeni tanımlanacak olan IP adres blokları kara listede (black list) olmayan adresler olacaktır. IP blokları her açıdan temiz (spamlı olmayacak, yasadışı amaçlar için kullanılmamış vb.) olacaktır.

**2.7.17.2.7** Yüklenici tahsis edeceği IP adres bloğuna dair tüm yapılandırmaları sözleşme kapsamında gerçekleştirecektir.

**2.7.17.2.8** Metro ethernet internet hizmeti hız kapasitesi talep halinde altyapı desteklediği durumda en fazla 72 (yetmiş iki) saat içerisinde arttırılacaktır.

**2.7.17.3** Veri Merkezleri Arası Bağlantı Hizmeti

**2.7.17.3.1** Yüklenicinin sağladığı veri merkezleri arasında erişim hızı 50 Mbit/s olan metro ethernet hizmeti sağlayacaktır.

**2.7.17.3.2** Ekte listesi bulunan diğer bağlantı hızlarının fiyatları teklifte detaylandırılacaktır. İDARE, önceden haber vererek hızları düşürebilir veya artırabilir.

**2.7.17.3.3** İstenilmesi durumunda bu bağlantıyı ikinci katman (L2) olarakta verebilmelidir.

**2.7.17.3.4** Teklif edilecek metro Ethernet hizmet altyapısı en az 1000 Mbit/s hızı destekleyecek kapasitede olacaktır.

**2.7.17.3.5** Her iki veri merkezinin kurulumu aşamasında veri senkranizasyonu için bağlantı hızı en yüksek seviyeye çıkartacaktır. Yüklenici bu hizmeti için ayrıca ücret almayacaktır.

**2.7.17.3.6** Yüklenici iki veri merkezi arasında sağladığı bağlantının yedekliliğinden sorumludur. Bir problem olması durumunda hiçbir müdahaleye gerek kalmadan ve kesinti olmadan bağlantının devamlılığını sağlamalıdır. Yüklenici bu hizmeti için ayrıca ücret almayacaktır.

**2.7.17.3.7** Yüklenici, sağladığı Metro Ethernet hizmeti için en fazla 5 dakikalık aralıklarla, günlük, haftalık, aylık ve yıllık olarak trafik miktarlarının izlenebileceği web ara yüzü (MRTG) sunacaktır.

**2.7.17.3.8** Metro ethernet internet hizmeti hız kapasitesi talep halinde altyapı desteklediği durumda en fazla 72 (yetmiş iki) saat içerisinde arttırılacaktır.

**2.7.17.4** Çok Noktadan Çok Noktaya (MPLS VPN) Erişim Hizmetleri

**2.7.17.4.1** Yüklenici, Çok Noktadan Çok Noktaya (MPLS VPN) erişim hizmetinin bu şartnamede yer alan hızlara göre ve belirtilmiş olan bakım garanti hükümlerine göre kesintisiz bir şekilde sözleşme süresi boyunca ve kapsamında temini, tesisi, bakımı, destek hizmetleri ve dokümantasyon işlerinin yapılmasını sağlayacaktır.

**2.7.17.4.2** Yüklenicinin sağlayacağı Merkezi ve Yedek veri Merkezlerinde Metro Ethernet internet hizmeti bu şartnamede belirtilmiş olan bakım garanti hükümlerine göre kesintisiz bir şekilde sözleşme süresi boyunca ve kapsamında temini, tesisi, bakımı, destek hizmetleri, dokümantasyon, hat durum analiz raporlarının alınabilmesini sağlayacaktır.

**2.7.17.4.3** Yüklenicinin Kuruma sağladığı çok noktadan çok noktaya erişim hizmeti internet üzerinden verilmeyecek olup ve internetten erişimlere tamamen kapalı olarak yetkisiz/dış erişimlerden arındırılmış şekilde sağlanacaktır.

**2.7.17.4.4** Teklif hazırlama aşamasında istekliler montaj mahallini tanımak, Çok Noktadan Çok Noktaya bağlantılar için kurulacak malzemelerin montaj yerlerini tespit etmek, ağ güzergâhlarını ve mesafelerini belirlemek amacı ile keşif yapacaklardır. İhalenin üzerinde kalması durumunda keşif yapılmamasından veya keşif yapıldığı halde farkına varılmamasından kaynaklanan zorluklar ve problemler yüklenici tarafından çözümlenecek, hiçbir şekilde ilave ücret talep edilmeyecektir.

**2.7.17.4.5** Kurum, kullanılacak Metro Ethernet internet data hattındaki olası hız değişimleri için ihtiyaca göre teklif edilen birim fiyatlar üzerinden sözleşme süresince artırma, eksiltme ve diğer değişiklikleri yapabilecektir.

**2.7.17.4.6** İşbu şartnamede bahsedilen hız değişimlerinin birim fiyat cetvelindeki hızlardan farklı olması durumunda, Yüklenici güncel tarifesini aşmamak kaydı ile talep edilen hız için teklifini İdareye sunacaktır. Sunulan teklifin kabul edilmesi durumunda sözleşme tasarısındaki şartlara bağlı kalarak iş artışı veya eksilişi yapılacaktır.

**2.7.17.4.7** İstekliler, şartname kapsamında verilen hizmetleri sağlamaya yetkili olduklarını gösterir Bilgi Teknolojileri ve İletişim Kurumu'ndan almış oldukları onaylı altyapı işletmecilik belgesini tekliflerinde sunacaktır.

**2.7.17.4.8** Yüklenici tarafından yapılacak işlemlerin takibi amacıyla proje yöneticisi atanmalıdır. Kurum proje yöneticisi değişikliği talep edebilir.

**2.7.17.4.9** Yüklenici sorunların bildirimi, çözümü için 7/24 ulaşılabilecek gerekli teknik personellerin iletişim numaralarını sözleşme imzalanmasından itibaren 5(beş) takvim gününde idareye yazılı olarak bildirmelidir.

**2.7.17.4.10** Yüklenici, Satış sonrası Teknik Hizmet Yönetimi sağlamak üzere bir yetkilinin atanmasını sağlayacaktır. Bu yetkili idarenin bildirmiş olduğu teknik arıza/taleplerin takibini ve planlı çalışma koordinasyonunu ücretsiz sağlayacaktır. Gerekli durumlarda kalıcı çözüm takibi ve iletişimini sağlayacaktır.

**2.7.17.4.11** Yüklenici, hizmet kapsamında verilecek olan tüm ürünlerin/malzemelerin sözleşme süresi içinde vereceği teknik destek karşılığında hiçbir ek ücret talebinde bulunmayacaktır.

**2.7.17.4.12** Yüklenici, İdare'ye arıza bildirimi için irtibat telefon numaralarını ve adreslerini sözleşmenin imzalandığı tarihinden itibaren en geç 2 (iki) gün içinde yazılı olarak bildirecektir. Herhangi bir arıza durumunda İdare, Yükleniciyle bu telefon numaraları aracılığıyla irtibat kuracaktır.

**2.7.17.4.13** Taşınma veya herhangi bir sebeple yüklenicinin telefon numarasının veya adresinin değişmesi durumunda Yüklenici İdare'ye yeni adres veya telefon numaralarını en geç 2 (iki) gün içerisinde yazılı olarak bildirecektir.

**2.7.17.4.14** Kurum, Yükleniciye garantisi kapsamına giren uygulamalar ile ilgili arıza bildirimi yaptıktan sonra yüklenici en geç 1 (bir) saat içerisinde arızaya müdahale etmeli ve sorunu en geç 1 (bir) gün içerisinde çözmelidir. Arıza kapsamında cihaz değişimleri kapsam dışındadır ve 48 saat içerisinde gerçekleştirilmektedir. Vendor firmalara açılan kayıtlarda geçen süreler kapsam dışındadır.

**2.7.17.4.15** Yüklenici, kullanılacak Metro Ethernet switchleri sözleşme süresi boyunca ücretsiz olarak temin edecektir.

**2.7.17.4.16** Yüklenicinin proje kapsamında temin edeceği tüm cihazlar kullanılmamış yeni ürün olmalıdır.

**2.7.17.4.17** Yüklenici, aylık hizmet bedeli dışında bağlantı veya nakil vb. işlemler için ücret talep etmeyecektir.

**2.7.17.4.18** Her bir birimde bağlantının eksiksiz olarak tamamlanmasından ve çalışır duruma getirilmesinden sonra mevcut durumda kullanılan data devrelerinin iptal işlemi İdare tarafından yapılacaktır.

**2.7.17.4.19** Yüklenici MPLS VPN omurgası aylık erişilebilirlik oranı aynı POP noktasında en az %99,8 olacaktır.

**2.7.17.4.20** Muayene esnasında meydana gelebilecek her türlü kaza ve hasardan yüklenici sorumlu olacaktır.

**2.7.17.4.21** Yüklenici Merkezi veri merkezi ile Çobançeşme yerleşkesi arasında erişim hızı 50 Mbit/s olan MPLS VPN hizmeti sağlayacaktır.

**2.7.17.4.22** Yüklenici Merkezi veri merkezinin kurulumu aşamasında veri senkranizasyonu için Çobançeşme yerleşkesi ile bağlantı hızı en yüksek seviyeye çıkartacaktır. Yüklenici bu hizmeti için ayrıca ücret almayacaktır.

**2.7.17.4.23** Bazı bölgelerden yapılacak yedek MPLS VPN hizmeti için, Yedek veri Merkezinde gerekli altyapı yüklenici tarafından hazırlanmalıdır

**2.7.17.4.24** MPLS VPN hizmeti hızları şu şekilde olmalıdır;

**2.7.17.4.24.1** TİM, İİB, İMMİB, İTKİB lokasyonlarından 20 Mbit/s

**2.7.17.4.24.2** AKİB, BAİB, DAİB, DENİB, DKİB, EİB, GAİB, KİB, OAİB, UİB lokasyonlarından 10 Mbit/s.

## 2.7.18 GSM Üzerinden Yedek Bağlantı Hizmeti ve Detaylar

**2.7.18.1** GSM şebekesi üzerinden kablosuz internet hizmeti sağlanacaktır.

**2.7.18.2** Bağlantı mümkünse 4.5G, yoksa 3G, her iki teknoloji olmayan bölgelerde GPRS destekleyecektir.

**2.7.18.3** Birliklere ait tüm GSM internet bağlantıları ayrı bağımsız bir APN ağ olacaktır. Bu APN TİM veri merkezine IPSec VPN ile bağlanacaktır.

## 2.7.19 DDOS ve Detaylar

**2.7.19.1** Yüklenici tarafından, Hizmet Alanın internet trafiği üzerinde "DDoS Saldırı Önleme Hizmeti" verilecektir. İnternet trafiğine DDoS saldırısı olması durumunda, saldırı trafiği, kullanıcı cihazlarına ulaşmadan önce önlenerek temizlenecektir.

**2.7.19.2** Yüklenici temin edilecek olan internet devresin 7/24 gerçek zamanlı DDOS saldırılarından koruyacak hizmeti sağlayacaktır. Bu hizmet trafiğin gerçek zamanlı izlenmesine dayanmalıdır. DDOS atak koruma hizmetinde sürekli olarak koruma sağlanıp trafik üzerinde anormallikler anında tespit edilip otomatik koruma çok hızlı bir şekilde gerçekleştirilmelidir.

**2.7.19.3** Yurtdışı veya dışardan gelecek volumetrik ataklara karşı koruma sağlanacaktır.

**2.7.19.4** DDoS saldırı önleme hizmeti hacimli büyük volumetrik ataklara karşı koruma sağlayacaktır.

**2.7.19.5** DDOS koruması kapsamında oluşan belirli alarmlar (atak alarmları vb.) kurumda ilgili kişilere eposta olarak gönderilecektir.

## 2.7.20 Genel Hizmetler ve Detaylar

**2.7.20.1** Yüklenici verdiği bütün hizmetlerin envanterinin tek bir yerden görüntülenebildiği bir portal sağlamalıdır. Bu portalden envanter raporu çekilebilmeli, arıza/talep bildirim yapılabilmeli ve yapılan bildirimler takip edilebilmelidir.

## 2.8 YÖNETİLEN HİZMETLER

### 2.8.1 Proje Yönetimi ve Detaylar

**2.8.1.1** Sözleşmenin imzalanmasını takiben 15 gün içerisinde YÜKLENİCİ, Proje Planını İDARE'nin onayına sunacaktır.

**2.8.1.2** İDARE, YÜKLENİCİ tarafından sunulan planı 15 gün içerisinde onaylayacaktır veya düzeltilmesi için geribildirimde bulunacaktır.

**2.8.1.3** YÜKLENİCİ, ihale kapsamında sağlanacak altyapıların kurulumu için Proje Yöneticisi olarak en az bir kişi görevlendirecektir.

**2.8.1.4** YÜKLENİCİ, ihale kapsamında sağlanacak altyapılar hizmete alındıktan sonra hizmetlerin sağlıklı yürütülebilmesi ayrıca için bir Teknik Proje Yöneticisi atayacaktır. Teknik Proje Yöneticisi, sağlanan hizmetler ile ilgili olarak gerçekleştireceği haftalık toplantılarda sağlanan hizmetleri İDARE ile değerlendirecek ve hizmetlerin iyileştirmesi konusunda iyileştirme süreçlerini işletecektir.

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

I. Kapsam ve Vizyon
II. Planlama
III. Geliştirme
IV. Kararlı Hale Getirme
V. Yaygınlaştırma

**2.8.1.6** İş Başında Eğitim (On-the-job training) Tüm çalışmalarda (her bir proje/danışmanlık için ayrı ayrı olacak şekilde) aşağıdaki dokümanlar üretilmeli ve teslim edilmelidir.

I. Kapsam ve Vizyon dokümanı
II. Proje planı (Sürekli güncellenecek – mpp ve xlsx formatlarında)
III. Risk dokümanı (Sürekli güncellenecek)
IV. Analiz dokümanı
V. Planlama ve tasarım dokümanı
VI. Geçiş esnasında gerekecek prosedürler ve kontrol listeleri
VII. Haftalık ilerleme durum raporu

**2.8.1.7** Tüm çalışmalarda aşağıdaki durumlarda toplantı yapılması gerekecektir.

I. Alt proje başlangıçlarında
II. Kriz anında
III. Tasarım ve geçişlerde gerektiği zaman
IV. İdare talep ettiği zaman

## 2.9 BAKIM VE YÖNETİLEN HİZMETLERİ

### 2.9.1 Bakım Şartları

**2.9.1.1** Tüm sistemin bakımı firma tarafından yapılacaktır.

**2.9.1.2** Yüklenici ihale kapsamında iki sistem odasının bakımını yapacaktır.

**2.9.1.3** Bakım kapsamına, bu şartname ile alınacak tüm ürünler, bu ürünler üzerinde çalışan sanal sunucular, birliklerden veri merkezine getirilecek sunucu ve depolama üniteleri ve bakım süresince alınabilecek veri depolama üniteleri, sunucular, anahtarlar, router cihazları, güvenlik duvarı ve sunucular üzerinde çalışan sanal sunucular dâhildir.

**2.9.1.4** Sistemlerin bakımı 7x24 olacaktır. Yüklenici sistemleri vardiyalı sistemle 7x24 izleyecektir. Bunun sağlanabilmesi için firmanın 3 vardiya çalışan personeli olacaktır. Arıza durumunda müdahale hemen yapılacak, gerekirse ilgili kişi ve firmalara haber verilecektir. İzlenen sistemlerle ilgili 8 saatte bir, yapılan işlemlerle ilgili günlük rapor düzenli olarak Bilgi İşleme iletilecektir.

**2.9.1.5** İzleyen kişilerin bilgileri Kuruma gönderilecektir. Değişiklik olması durumunda kişi bilgileri önceden Kuruma iletilecektir.

**2.9.1.6** Firmanın firewall, sanallaştırma, ağ sistemleri ile ilgili sertifikalı uzman personeli bulunacaktır. Gerekli durumlarda bu personel ile sistemlere destek verecektir. Bu personellerin önerilen firewall cihazları, önerilen switch cihazları, Microsoft sistemleri, sanallaştırma sistemleri ile ilgili uluslararası geçerli sertifikaları olacaktır.

**2.9.1.7** Bakım kapsamında donanım arızası olması durumunda, donanım garantisi kapsamında ilgili firmalara kayıt açmak, ürünün garanti kapsamında değişikliğinin yapılması için takip yüklenicinin sorumluluğundadır.

**2.9.1.8** Sistemlerin güncellenmesi yüklenicinin sorumluluğundadır. Yüklenici planlamasını yaparak İdareye haber verecek ve kesinti olmadan veya İdarenin onayı ile minimum kesinti ile güncellemeleri yapacaktır.

**2.9.1.9** Arızalı ünitelerin firma servis merkezinde onarılmasının gerektiği durumlarda, oluşabilecek her türlü (nakliye, nakliye sigortası, nakliye hasarı vb.) masraf firma tarafından karşılanacaktır.

**2.9.1.10** Yüklenici, ihtiyaçları doğrultusunda Kurumun sistem tasarımını yapar, gerekli gördüğü değişiklikleri Kurum idaresine sunar ve onaylanmış değişikleri bir proje disiplini ile gerçekleştirir.

**2.9.1.11** Bakım ve arızaya müdahale anındaki her türlü yükümlülük ve sorumluluk yükleniciye aittir. Bu esnada yüklenici idarenin mal veya sistemlerine zarar vermesi halinde verilen zarar yükleniciden talep ve tahsil edilecektir.

**2.9.1.12** Yüklenici, arızaya müdahaleyi ve güncellemeleri, mutlaka Bilgi İşlem Müdürlüğünde görevli bir teknik yetkiliyi telefonla, yüz yüze veya eposta ile bilgilendirerek yapacaktır.

**2.9.1.13** Düzenli bakım veya arızaya müdahaleden sonra yüklenici firma yetkilisi tarafından düzenlenip; Bilgi İşlem Müdürlüğünce görevlendirilmiş teknik elamana imzalatılmak üzere; arızanın mahiyeti, yapılan işlem, değişen parçaların dökümünü gibi bilgileri kapsayan bir servis formu (bir nüshasını) Bilgi İşlem Müdürlüğüne teslim edilecektir.

**2.9.1.14** İleride, veri merkezlerinde konumlandırılacak yeni ürünler bakım anlaşmasına dahil olacaktır.

**2.9.1.15** Yüklenicinin web üzerinden arıza takip sistemi olacaktır. Web üzerinden arıza başvurularını yapmak için idareye en az iki kullanıcı hesabı (account) verilecektir. Bu başvuru her iki tarafça da kayıt altına alınacaktır.

**2.9.1.16** Arızalar mesai saatleri içinde yükleniciye Bilgi İşlem Müdürlüğünce belirlenen yetkili personel/personellerce (telefon, faks, Web ara yüzü veya eposta ile) bildirilecektir.

**2.9.1.17** İdarenin bünyesindeki birimlerin yerel alan ağındaki network performansında azalma olduğu takdirde, yüklenici performansın normal seviyeye gelmesi için gerekli çalışmayı yapacak ve problemi Bilgi İşlem yetkili personel/personeline yazılı ve sözlü rapor edecek ve giderecektir.

**2.9.1.18** Yüklenici, İdare tarafından istenmesi durumunda, yeni oluşturulacak olan İdarenin Politikaları çerçevesinde Veri Merkezindeki cihazlarındaki güvenlik problemlerine uygun çözümler önerecek ve gerekli konfigürasyonları yapacaktır.

**2.9.1.19** Her ay yapılacak bakım hizmetlerinde, sistemlerin doğru çalışıp çalışmadığına ve performansına bakılacaktır.

**2.9.1.20** Yapılan her türlü işlem, her türlü konfigürasyon değişiklikleri belgelendirilecektir.

**2.9.1.21** İşin gereklerine göre; aşağıdaki işleri yapmak firmanın sorumluluğundadır:

**2.9.1.21.1** Sistemlerin konfigürasyonunu yapmak,

**2.9.1.21.2** Yeni sunucu ihtiyacı olduğunda, gerekli sunucuların güvenliğini de planlayarak hazır hale getirmek,

**2.9.1.21.3** Kurumla çalışan diğer firmaların veri merkezi ve sunucu ihtiyaç taleplerini incelemek, firmayla görüşerek belirlenecek konfigürasyonu idarenin onayını alarak gerçekleştirmek,

**2.9.1.21.4** Arıza/problem durumunda müdahale edip gidermek, kök sebep analizlerini yapmak, gerekli Kurumsal bilgi Sistemlerine işlemek,

**2.9.1.21.5** Arıza dış bir faktör ile ilgili ise, ilgili komünikasyonu kurmak, arızayı/problemi çözdürmek, BT iş akışlarına göre zamanında üst idareyi bilgilendirmek.

**2.9.1.21.6** Sistemleri güncellemek ve güncel tutmak,

**2.9.1.21.7** Bakım kapsamında konfigürasyonları yedeklemek, Firmware'ler yeni versiyonları varsa güncellemek, (Firmware veya güncellemeler ücretli ise idarenin onayı alınacaktır.)

**2.9.1.21.8** Sistemlerin yazılım lisanslarının güncelliğini takip etmek, yenilenmesi ve/veya artırılması gereken lisanslar ile ilgili üst idareyi zamanında bilgilendirmek,

**2.9.1.21.9** Sistemleri optimize etmek ve sürekli optimize tutmak,

**2.9.1.21.10** Sistemlerin kapasite yönetimini yapmak, optimizasyon ve/veya arıza/problem yönetimi ile giderilemeyecek kapasite yetersizliklerinde BT iş akışlarına göre zamanında üst idareyi bilgilendirmek, yeterli kapasiteyi sektörel standartlarda fizibilite raporları ile tavsiye etmek, kurumu yönlendirmek,

**2.9.1.21.11** Sistemler ile ilgili yapılan tüm değişiklikleri dokümante etmek, tüm dokümantasyonu güncel tutmak,

**2.9.1.21.12** Sistemler ve ilgili konfigürasyonlarını Kurumun ilgili izleme sistemlerine tanımlamak ve bu sistemler üzerinden izlemek, gerekli güncellemeleri yapmak,

**2.9.1.21.13** Sistemler ve ilgili konfigürasyonlarını Kurumun ilgili log yönetim Sistemlerine entegre etmek ve gerekli hallerde yönetilen bu Sistemler veya izleme sistemleri üzerindeki loglar üzerinde incelemeleri yapmak, raporlar hazırlamak,

**2.9.1.21.14** Sistemlerin yedeklerini almak, düzenli geri yükleme testlerini yapmak,

**2.9.1.21.15** Yedekli çalışan Sistemlerin Kurum politika ve planları dahilinde yedeklilik testlerini yapmak,

**2.9.1.21.16** BT projeleri kapsamında başta analiz iş yükleri olmak üzere Sistem konfigürasyonlarına destek vermek.

**2.9.1.22** Yüklenici tarafından aylık testler yapılacaktır

**2.9.1.22.1** Yüklenici, ayda bir adam gün sunucular üzerinde performans testi yapacaktır.

**2.9.1.22.2** Her ay hangi sunucuların testi yapılacağı kurumla beraber kararlaştırılacaktır.

**2.9.1.22.3** Yüklenici, ayda dört adam gün penetrasyon testi yapacaktır. Her ay hangi sunucuların testi yapılacağı kurumla beraber kararlaştırılacaktır. Bu testler konusunda uzman TSE Onaylı Sızma Testi firmalarından birine yaptırılacaktır.

**2.9.1.22.4** Testler yapılırken kesinlikle son kullanıcı işlemlerinde genel performans kaybı olmayacaktır.

**2.9.1.22.5** Yüklenici, testler öncesi Bilgi İşlem Müdürlüğüne bilgi verecektir.

**2.9.1.22.6** Yüklenici, network ağının çalışırlığını test edip, tekrarlanan sorunların giderilmesinde etkin ve kalıcı çözümler planlayıp; kurulu network üzerinde optimizasyon (en iyileme) ve tuning (ince ayar) önerilerini raporlarında belirteceklerdir.

**2.9.1.22.7** Yüklenici, test sırasında Veri Merkezlerindeki ve dış lokasyonlarla Veri Merkezleri arasındaki ağ trafiğini analiz edecek hız önerilerini Bilgi İşlem'e sunacaktır. GÜVENLİK OPERASYONLARI MERKEZİ (SOC) HİZMETİ

## 2.9.2 Güvenlik Operasyonları Merkezi (SOC) Hizmeti

**2.9.2.1** Amaç ve Kapsam: Kurumun sahip olduğu bilişim sistemlerindeki güvenliğin arttırılması, mevcut olan güvenlik zafiyetlerinin tespit edilip, gerekli aksiyonların alınarak olası iç ve dış güvenlik tehditlere karşı bilgi güvenliğinin ve güvenlik farkındalığının arttırılması, regülasyonlara, mevzuatlara ve kanunlara uyumlu bir şekilde işletilebilir seviyeye getirilmesinin sağlanması için hizmet alımı yapılacaktır. Kapsam aşağıdaki maddeleri içerecektir;

**2.9.2.1.1** Kurumun sistemlerinden gelen alarmların gerçek zamanlı olarak 7/24 takip edilmesi ve izlenmesi, kapsamlı ve zengin siber tehdit veritabanlarında değerlendirilerek, sağlıklı ve hızlı bir şekilde gereken durumlarda söz konusu güvenlik olaylarının kurum içindeki ilgili ekiplere/kişilere yönlendirilmesi

**2.9.2.1.2** Güvenlik olaylarının raporlanması ve kayıt altına alınması

**2.9.2.1.3** SOC ekibinin planlaması doğrultusunda iyileştirme çalışmalarında ve oluşabilecek kritik durumlarda uzaktan ve yerinde desteğin verilmesi,

**2.9.2.1.4** Kurumun mevcut topolojisine uygun olarak korelasyonlarının yazılması

**2.9.2.1.5** Zararlı Yazılım Analizi ve Siber İstihbarat Hizmetlerinin verilmesi ve çıktılarına istinaden korelasyon kurallarının sürekli iyileştirilerek güncel tutulması,

**2.9.2.1.6** Olay analiz ve müdahale hizmetlerinin bir parçası olarak, siber güvenlik tehditlerinin başında yer alan kötücül yazılımlar, bu konuda uzmanlaşmış ekiplerce en son teknik ve araçlar kullanılarak statik ve dinamik olarak analiz edilmeli, kurum bilgi sisteminde bıraktığı zararlar tespit edilmelidir.

**2.9.2.1.7** Teknik Şartlar

**2.9.2.1.8** Yetki Yönetimi ve Loglama

**2.9.2.1.8.1** Kurum tarafından alınacak SIEM çözümü kullanılacaktır.

**2.9.2.1.8.2** Kullanılan SIEM çözümü kullanıcı işlemlerine ilişkin log kayıtlarını saklamalıdır.

**2.9.2.1.9** Sistem Yönetimi

I. 7/24 sistem performans takibi yapılmalıdır. Bu takip kapsamında en azından CPU, Memory, Storage ve EPS değerleri yer almalıdır.
II. Kurumun talep ettiği raporlar oluşturulmalıdır.
III. Kurumun talep ettiği alarmlar oluşturulmalıdır.
IV. Kurumun talep ettiği korelasyon kuralları yazılmalıdır.
V. Kurumun talep ettiği yeni log kaynaklarının entegrasyonu sağlanmalıdır.
VI. 24 saat boyunca log göndermeyen kaynaklara ilişkin bilgi paylaşımı ve kontroller yapılmalıdır.
VII. Planlanan ve kesinti riski yaratabilecek sistem güncellemeleri, upgrade çalışmaları müşteri ile çalışmadan en az 3 iş günü öncesinden paylaşılmalıdır.

**2.9.2.1.10** Sistem Bakımı

**2.9.2.1.10.1** Yılda en az iki defa SIEM sağlık tarama hizmeti sunulur ve tarama çıktıları bir rapor olarak müşteri ile müşteri lokasyonunda paylaşılmalıdır.

**2.9.2.1.10.2** Raporda donanım, yazılım, network, backup, zaman damgası entegrasyonu, entegre log kaynakları, aktif korelasyon kuralları ve alarm oluşumu ile ilgili mevcut durum ile önerilen iyileştirme aksiyonları ve planları paylaşılmalıdır.

**2.9.2.1.10.3** Sistemde oluşan problemlere SLA'lere uyumlu bir şekilde müdahale edilmelidir.

**2.9.2.1.10.4** Sistemde oluşan ve çözümlenemeyen problemlerle ilgili olarak üretici ile case takibi yapmalıdır.

**2.9.2.1.10.5** Yılda bir kez upgrade çalışması yapılabilmelidir.

## 2.9.3 SOC İzleme

**2.9.3.1** SOC İzleme Detayları

**2.9.3.1.1** Oluşan tüm alarmlar 7/24 takip edilmeli ve incelenmelidir. Aksiyon alınması gereken ya da takip edilmesi gereken konularla ilgili olarak müşteri bilgilendirilmelidir.

**2.9.3.1.2** Aksiyon alınması gerekmeyen ya da müşteri tarafından normal olarak belirtilen alarmlar müşterinin ihtiyaçları doğrultusunda fine tune edilmelidir.

**2.9.3.1.3** Kurum ile yapılacak çalışmalarla korunması gereken kritik altyapılar, kritik kullanıcılar belirlenmelidir. Bu altyapı ve kullanıcılara yönelik alarmların kritiklik seviyesi yükseltilmelidir ve yakından takip edilmelidir.

**2.9.3.1.4** Kuruma sunulan SOC hizmetine ilişkin olarak her ay müşteri lokasyonunda bilgi paylaşımı için bir sunum yapılmalıdır. Bu sunumda yeni entegre edilen log kaynakları, yeni yazılan kurallar, offense trendi, eps trendi, bildirim trendi, saldırı karakteristikleri ve alınması önerilen aksiyonlar paylaşılmalıdır.

**2.9.3.1.5** SIEM altyapısında oluşturulan alarmlar farklı siber istihbarat servislerinden alınan bilgilerle zenginleştirilmelidir.

## 2.9.4 Siber İstihbarat

**2.9.4.1** Siber İstihbarat Detayları

**2.9.4.1.1** Hizmet kapsamında Kurum özelinde gelişmiş siber istihbarat servisi sağlanır (iç kaynak ve/veya anlaşmalı olunan alanında uzman bir firma üzerinden) ve SOC operasyonunun sürekli olarak bu veriyle güncellenmesi hedeflenir.

**2.9.4.1.2** Kurum IP blokları sistem üzerinden anomalilere karşı izlenmelidir.

**2.9.4.1.3** Kurum ile ilgili darkweb taramaları yapılmalı ve tespit edilen bulgular raporlanmalıdır.

**2.9.4.1.4** Kurumun sektörü ile ilgili siber istihbaratlar ve saldırı analizleri paylaşılmalıdır.

**2.9.4.1.5** Kurumun ilgili phishing ve cybersquatting aktiviteleri izlenmeli ve raporlanmalıdır.

**2.9.4.1.6** Sosyal medya kanalları üzerinde müşterinin markasına yönelik uygunsuz durumlar izlenmeli ve raporlanmalıdır.

**2.9.4.1.7** 20 Adet Domain, 10 adet IP adresi izlenecektir.

## 2.9.5 Yönetilen Hizmetler

**2.9.5.1.1** Alınan tüm ürünlerin Yönetimi Hizmetlerinin PMP Metodolojisi ve ITIL süreçleri doğrultusunda yönetilmesi ve operasyonun sürekliliği firma tarafından sağlanacaktır.

**2.9.5.1.2** Sisteme dahil olan her birliğin Veri Merkezindeki sunucu altyapısının belirlenmesi ve sistemlerin taşınması ve işletilmesi hizmetleri verilecektir.

**2.9.5.1.3** Yönetilebilir hizmetler konusunda alınacak hizmet başlıkları aşağıdaki şekildedir:

**2.9.5.1.3.1** Veri Merkezi Anahtarları Yönetimi
**2.9.5.1.3.2** Güvenlik duvarı yönetimi
**2.9.5.1.3.3** Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü Yönetimi
**2.9.5.1.3.4** SIEM ürünü ayda bir log alma ve korelasyon kontrolü
**2.9.5.1.3.5** E-posta Güvenliği Ürünü Yönetimi
**2.9.5.1.3.6** Web Güvenliği Ürünü Yönetimi
**2.9.5.1.3.7** Sunucu Güvenliği Ürünü Yönetimi
**2.9.5.1.3.8** Saldırı Yüzeyi Yönetimi Ürünü Yönetimi
**2.9.5.1.3.9** Sanallaştırma Yazılımı Yönetimi
**2.9.5.1.3.10** Birlikler tarafından talep edilen sanal sunucuların kurulması ve kaynak yönetimi
**2.9.5.1.3.11** Yedekleme Yazılımı Yönetimi
**2.9.5.1.3.12** Yedek stratejilerinin belirlenmesi
**2.9.5.1.3.13** Yedekleme görevlerinin eklenmesi ve izlenmesi
**2.9.5.1.3.14** Replikasyon görevlerinin eklenmesi ve izlenmesi
**2.9.5.1.3.15** Disaster anında restore işleminin gerçekleştirilmesi
**2.9.5.1.3.16** 6 ayda bir yedekten dönme testlerinin yapılması
**2.9.5.1.3.17** Sunucu İşletim Sistemi Kurulumu
**2.9.5.1.3.18** Sunucu İşletim Sistemi Güncellemelerinin yapılması
**2.9.5.1.3.19** Loglama ve Raporlama Ürünü Yönetimi
**2.9.5.1.3.20** İzleme (Monitoring) Yazılımı Yönetimi
**2.9.5.1.3.21** Çok Faktörlü Kimlik Doğrulama Yazılımı Yönetimi
**2.9.5.1.3.22** Ayrıcalıklı Erişim Yönetimi (PAM) Ürünü Yönetimi
**2.9.5.1.3.23** Web Zafiyet Tarama Yazılımı Yönetimi
**2.9.5.1.3.24** AD Obje (kullanıcı ve grupların) Yönetimi
**2.9.5.1.3.25** Organizational Unit (OU) Yönetimi
**2.9.5.1.3.26** DNS (Domain Name System) Yönetimi
**2.9.5.1.3.27** Group Policy Object Yönetimi
**2.9.5.1.3.28** Genel Katalog (Global Katalog) Yönetimi
**2.9.5.1.3.29** Site ve Subnet Yönetimi
**2.9.5.1.3.30** Yetkilendirme Yönetimi
**2.9.5.1.3.31** EPosta Yönetimi
**2.9.5.1.3.32** Fiziksel sunucu yönetimi
**2.9.5.1.3.33** Fiziksel depolama ünitesi yönetimi
**2.9.5.1.3.34** Yılda bir kez FKM test işlemi
**2.9.5.1.3.35** Mevcut sunucu talepleri ile ilgilenme

**2.9.5.1.4** Personel Bulundurma başlıkları aşağıdaki şekildedir:

**2.9.5.1.4.1** YÜKLENİCİ, sistemlerin takibi ve iyileştirilmesi için sunucu ve sanallaştırma konusunda en az 5 (beş) yıl deneyimli ve uzmanlık alanında sertifikası olan bir personeli haftada 3 gün mesai saatleri içinde TİM Bilgi İşlem Müdürlüğünde bu sistemlerin bakımı için çalıştıracaktır.

**2.9.5.1.4.2** YÜKLENİCİ, tüm lokasyonlarda görevlendirilecek olan personel bilgilerini, personel işe başlamadan önce özgeçmişi ile birlikte İDARE'ye bildirilecek ve İDARE'nin onay vermesi halinde görevlendirme sağlanacaktır.

**2.9.5.1.4.3** YÜKLENİCİ, tüm lokasyonlarda görevlendirilecek personelin bütün evrak, çalışma vb. izinlerini, iş sağlığı vb. eğitimlerini, sosyal ve özlük haklarını, işyerinde kullanacağı teknik cihazlarını ve ulaşım hizmetlerini kendisi karşılayacaktır. İDARE, personelin kanuni sorumlulukları ile ilgili hiçbir şekilde sorumlu tutulmayacaktır.

**2.9.5.1.4.4** YÜKLENİCİ ve İDARE ayrı ayrı, tüm lokasyonlarda görevlendirilecek personelin devam takibi, yoklama sistemi ile aylık giriş-çıkış cetvelini takip edecektir. YÜKLENİCİ, takip çizelgesini evrak olarak fatura ile birlikte İDARE'ye sunacaktır. Her iki çizelgede mutabık kalınması durumunda fatura işleme alınacaktır.

**2.9.5.1.4.5** YÜKLENİCİ, tüm lokasyonlarda görevlendirilecek personelin izin, rapor vb. gibi özlük haklarından kaynaklanan işe gelmemesi durumunda yerine yine aynı seviyede şartları sağlayan profesyonel bilgiye ve tecrübeye sahip bir personel görevlendirecektir. Görevlendirilen geçici personeller de aynı şekilde yoklama sistemi ile aylık giriş-çıkış cetveli ile takip edilecektir.

## 2.10 SERVİS SEVİYESİ ÖZELLİKLERİ

### 2.10.1 Servis Seviyesi Özellikleri Ve Detayları

**2.10.1.1** YÜKLENİCİ sağlayacağı hizmetler için aşağıdaki çağrı önceliklendirmesine uygun altyapıya sahip olmalıdır.

| | | Etki | | | |
|---|---|---|---|---|---|
| | | 1 – Enterprise (Çok Yaygın) | 2 – Multiple Sites (Geniş) | 3 – Department (Orta) | 4 – User (Az) |
| Aciliyet | 1 – Kritik Acil | 1 | 1 | 2 | 2 |
| | 2 – Yüksek | 1 | 2 | 2 | 3 |
| | 3 – Orta | 2 | 2 | 3 | 3 |
| | 4 – Düşük | 2 | 3 | 3 | 4 |

| Öncelik | | Açıklama |
|---|---|---|
| Kritik Acil | (1) | Bu skalaya giren olay kayıtlarından Majör olanları Majör Olay kaydı olarak değerlendirilir. Diğerleri Kritik seviyesinde değerlendirilir. Önemli iş fonksiyonun yerine getirilememesi, hizmete çoğunluk kullanıcının erişememesi, müşteri/para/itibar kaybı yaratan durumlar bu kategoride değerlendirilir. |
| Acil | (2) | Olay kaydı Majör olay olabilme ihtimaline karşı bir kez daha değerlendirilir. Bu değerlendirme sonucunda gerekirse Majör Olay statüsüne yükseltilir. Majör sınıfına yükseltilmeyen kayıtlar için öncelikli müdahale ve kaynak ataması yapılır. Sorun sırasında ve çözüm sonrasında müşteri bilgilendirilir. Benzer bir durumun oluşma ihtimaline karşı bir süre sistem izlemesi yapılır. Bu kapsama, sistemin bazı fonksiyonlarının doğru çalışmaması ya da yavaşlaması (operasyonların kısmen etkilenmesi ve durması). Sistemin bakım ve işletim fonksiyonlarının operasyonu engelleyecek seviyede çalışması. Sistemin planlanan kapasiteyi ve/veya performansı karşılayamaması yüzünden oluşan durumlar. |
| Orta | (3) | Normal olarak önceliklendirilir. Kaynak ataması ve zamanlandırma ilgili birimin iş yüküne göre belirlenebilir. Çözüm sonrası kullanıcı bildirimi yapılır. |
| Düşük | (4) | Önceliklendirme yapılmaz. İlgili birimin iş yüküne göre çözüm çalışmasına başlanır. İş yükünün yüksek olması durumlarında daha sonra kontrol edilmek üzere bekletilebilir. Çözüm sonrası ek aksiyon alınmaz. Hatırlatma ya da kontrol amaçlıdır. |

5.2.1.1. Yüklenici sağladığı hizmetler için aşağıdaki müdahale sürelerine uymalıdır.

| SLA | Hedef Değer |
|---|---|
| Kritik Acil Öncelikli Olay Müdahale Süresi | <= 60 dakika |
| Acil Öncelikli Olay Müdahale Süresi | <= 120 dakika |
| Orta Öncelikli Olay Müdahale Süresi | <= 4 saat |
| Düşük Öncelikli Olay Müdahale Süresi | <= 8 saat |

**2.10.1.2** Planlı bakım süreleri (Kesintisiz Güç Kaynağı Bakımı, Veritabanı bakımı, Patchlerin yüklenmesi v.b.) kesinti süresi olarak ele alınamaz.

**2.10.1.3** Yüklenici, İDARE'nin kasıtlı hareketi, hatası veya ihmali durumunda sorumluluklarını yerine getirmemesi ve Müşteri tarafından getirilen üçüncü şahısların müdahalesi nedeniyle meydana gelen problemlerden kaynaklanan arızaları bulmak ve/veya onarmak için yaptığı çalışmalar ve değiştirilen ekipman için, karşılıklı mutabakat ile Müşteri'den ücret almak hakkına sahip olacaktır ve bu sürede sistemde meydana gelecek kesintiler hizmet kesintisi olarak değerlendirilmeyecektir.

**2.10.1.4** Donanım, yazılım ve sistem için kullanılan arabirimleri üreten firmalardan, kaynaklanan hataların çözümü için geçen süre, üretici firma bu hatayı üstlendiğini belgelerse veya yüklenici ve İdare üretici firmadan kaynaklandığı konusunda mutabakata varırsa, kesinti olarak değerlendirilmez.

**2.10.1.5** Belirtilen hizmet düzeyleri yazılım sağlayıcısının (Microsoft, vb.) desteklediği versiyonlar için geçerlidir. Yazılım sağlayıcısının üretim hatasından kaynaklanan sorunlar, hizmet düzeyi kesintisi olarak değerlendirilmez.

**2.10.1.6** Bölümde belirtilen servis seviyelerine ulaşılamaması halinde, yükleniciye cezai yaptırımlar uygulanacaktır. Uygulanacak ceza miktarı, belirlenen ve ölçülen servis seviyelerinin ve bunların sağlanamama sürelerinin bileşimi olarak hesaplanacaktır. İDARE'ye sunulan hizmetler 7*24 verilecektir. Aylık Hizmet Toplam Süresi 720 saattir. Bu hizmetin süreklilik oranı Yüklenici tarafından garanti edilmelidir.

**2.10.1.7** Aylık ceza miktarı aşağıdaki formüle göre hesaplanacaktır;

| | | |
|---|---|---|
| HB | : | Aylık Altyapı Hizmet Bedeli |
| MAS | : | Müdahale Aşım Süresi |
| ÖN | : | Öncelik Seviyesi |
| **Ceza miktarı = HB * (MAS/ÖN) * (%0,15)** | | |

**2.10.1.8** Metrikler aylık olarak ölçülüp raporlanacaktır. Anlaşılan servis seviyelerine ulaşılamaması durumunda, ulaşılamayan her bir servis seviyesi için, aylık fatura bedelinin %0, 5'i oranında ceza uygulanacaktır.

## 2.11 KURULUMLAR

### 2.11.1 Sistem Altyapısı Kurulum

**2.11.1.1 Fiziksel Ürünlerin Kurulumu Genel Başlıklar;**

**2.11.1.1.1** Yüklenici kuruluma başlamadan önce proje yöneticisi tayin edip yönetime bildirecektir.

**2.11.1.1.2** Proje yöneticisi ve proje teknik sorumlusu ihale konusu ve/veya benzer işlerde çalışmış olmalıdır.

**2.11.1.1.3** Yönetimin proje yöneticisini/proje teknik sorumlusunu değiştirme hakkı saklıdır.

**2.11.1.1.4** Sistem için gerekli olan tüm cihazlar yüklenici tarafından kurulacak, konfigürasyonu yapılacak ve çalışır halde teslim edilecektir.

**2.11.1.1.5** Tasarım, kurulum ve yapılandırma hizmetleri daha önce ihale konusu işler ve/veya benzer işlerde çalışmış, konusunda uzman personeller tarafından verilecektir.

**2.11.1.1.6** Teklif edilen tim bu ürünlerin işbu şartname kapsamındaki istekleri yerine getirecek şekilde kurulumu ve sorunsuz şekilde devreye alınması için gerekli tüm ekipmanları (Montaj kitleri, güç kabloları, PDU, bakır ve fiber data kabloları vb.) yüklenici tarafından sağlanacaktır.

**2.11.1.1.7** Kurulum ile ilgili tüm ek malzemeler yüklenici tarafından karşılanacaktır.

**2.11.1.1.8** Kurulum donanım üreticilerinin tavsiye ettiği en iyi kurulum (Best Practice) yapısına uygun olarak yapılacaktır.

**2.11.1.1.9** Cihazlar montaj sırasında mevcut kabinler içerisinde yedekli olarak konumlandırılmalıdırlar.

**2.11.1.1.10** Kablolama düzenleri hem düzgün hem de kolay müdahale edilebilir olmalıdır.

**2.11.1.1.11** Yüklenici, gereken tüm ekipmanların kolay okunabilir, anlaşılabilir ve takip edilebilir şekilde etiketlemesini yapacaktır.

**2.11.1.1.12** Cihazlara uzak erişimde güvensiz protokoller devre dışı bırakılacaktır.

**2.11.1.1.13** Cihazlara uzak kullanıcı hesaplarının güvenliği sağlanacaktır.

**2.11.1.1.14** Yüklenici Sistemin tüm bileşenlerine düzenli olarak bakım yapar ve optimum performans için ince ayar yapar.

**2.11.1.1.15** Yüklenici, Sistem üzerinde yapılacak, donanımsal veya yazılımsal tüm değişikliklerin yönetiminden sorumludur.

**2.11.1.1.16** Yüklenici, işbu şartname kapsamında, Operasyon hizmetini verdiği tüm sistemler için detaylı topoloji dokümantasyonu hazırlar ve sürekli güncel tutar.

**2.11.1.1.17** Dokümantasyonun yeterliliği Kurum yetkililerinin onayına tabidir.

**2.11.1.2 Fiziksel Sunucular;**

**2.11.1.2.1** Cihazların management ara yüzleri en güncel halleri ile teslim edilecektir.

**2.11.1.2.2** Cihaz üzerinde yer alan disklerin gerekli RAID konfigürasyonları yapılacaktır.

**2.11.1.2.3** Cihazların network bağlantıları 10/40/100Gbps bağlantı hızı ile gerçekleştirilecektir.

**2.11.1.2.4** Cihaz management bağlantısı ayrı bir port üzerinden gerçekleştirilecektir.

**2.11.1.3 Depolama Ürünleri;**

**2.11.1.3.1** Cihazların fiziksel sunucular ile bağlantıları SAN Swtich aracılığı ile fiber kablolar üzerinden gerçekleştirilecektir.

**2.11.1.3.2** Gerekli RAID konfigürasyonları gerçekleştirilecektir. Spare disk planlaması yapılacaktır.

**2.11.1.3.3** Cihaz management bağlantısı ayrı bir port üzerinden gerçekleştirilecektir.

**2.11.1.3.4** Yönetimin talep edeceği ihtiyaçlara binaen LUN tanımlamaları yapılacaktır.

**2.11.1.4 Sanallaştırma Sistemi;**

**2.11.1.4.1** Daha önce Fiziksel kurulumu yapılan sunucular üzerine sanallaştırma yazılımının en son versiyonu yüklenecektir.

**2.11.1.4.2** Sanallaştırma yazılımının güncellemeleri yüklenir ve yüklenici tarafından takip edilecektir.

**2.11.1.4.3** Kurulum tamamlandıktan sonra sanallaştırma yazılımının sunucularının IP'leri DNS sunucusu üzerinde sabitlenecektir.

**2.11.1.4.4** Sanallaştırma sisteminin NTP yapılandırmaları ayarlanacaktır.

**2.11.1.4.5** Sanallaştırma sunucularının yönetmesi için Sanallaştırma sunucusu yöneticisi yazılımı kurulumu yapılacaktır.

**2.11.1.4.6** Sanallaştırma sunucusu yöneticisi üzerine yönetebilmesi için sanallaştırma sunucuları eklenecektir.

**2.11.1.4.7** Sanallaştırma sunucusu yöneticisi üzerinde yüksek erişilebilirlik ve yük dağılımı gibi servisler devreye alınacaktır.

**2.11.1.4.8** Sanallaştırma sunucusu yöneticisi üzerinden platform da kullanılacak olan kaynaklar tanımlanacaktır. (FC, iSCSI, NFS vs.)

**2.11.1.4.9** Misafir işletim sistemleri sanallaştırama sunucusu üzerinde kurulumu yapılır. Kaynaklar ilk kurulumda belirtilebileceği gibi sonrasında artırma işlemi yapılabilir.

**2.11.1.4.10** Belirli kişilerin erişimleri ve belli sunucuları yönetmesi vb. işlemler Sanallaştırma sunucusu yöneticisi üzerinden ayarlanır.

**2.11.1.4.11** Misafir işletim sistemlerinin performansı Ram, CPU, Harddisk gibi parametreler anlık ve geriye dönük olarak Sanallaştırma sunucusu yöneticisi tarafından izlenir.

**2.11.1.5 İşletim Sistemi;** Yüklenici, Kuruma Kurulum Hizmeti verir. Sistem Yönetim Hizmeti, Sistemin sunucu/rol bazında büyümesi/genişlemesi veya konsolidasyonu/küçülmesi gibi yapısal (aynı zamanda Majör) değişiklik gerektiren, analiz, tasarım, kurulum ve migrasyon türü iş yüklerinden oluşan hizmet türüdür. Yüklenici bu hizmet kapsamında aşağıdaki konulardan sorumlu olacaktır;

**2.11.1.5.1** Yüklenecek olan işletim sistemlerinin kendi sürümleri içinde güncel olanı tercih edilecektir.

**2.11.1.5.2** Yüklenici, sistemin bileşenlerinin üreticisi tarafından yayınlanan kritik ve güvenlik yamalarını düzenli olarak sisteme geçer, yama yönetimini yapar.

**2.11.1.5.3** Yüklenici Sistemin kapasite yönetimini yapar. Aynı türden bileşenleri arasında yük dengesini sağlamak, Kurum yönetimi ile silinmesinde mutabık kalınan dosya yüklerini silmek ve yer açmak ve Kurumu ek kapasite ihtiyacı konusunda, Sistemin işleyişini aksatmayacak, yavaşlatmayacak süre öncesinden bilgilendirmek ve kapasite talebinde bulunmak Yüklenicinin sorumluluğundadır.

**2.11.1.5.4** Yüklenici onaylanmış hedef mimari kurulumunu gerçekleştirecektir. Sistemin tüm bileşenlerinin kurulum sorumluluğu Yükleniciye aittir.

**2.11.1.5.5** Yalnızca Yüklenici Canlı ortamlarda Sistemsel değişiklik yapabilir. Sistemsel değişiklik, Sistemin donanım ve/veya yazılımsal herhangi bir bileşenin konfigürasyon ya da kaynağının veya bir fonksiyonunun değiştirilmesi demektir.

**2.11.1.6 E-posta Sunucusu;**

**2.11.1.6.1** E-Posta sunucu/sunucularının kurulacağı işletim sistemi üzerinde kaynak ayarlaması ihtiyaca göre uygulamanın hesaplama aracı ile planlanacaktır.

**2.11.1.6.2** İhtiyaç olması durumunda işletim sistemlerini kapatmadan kaynak artırımı yapılabilmelidir.

**2.11.1.6.3** Sunucularda client iletişimleri ile sunucuların kendi aralarındaki iletişim için en az iki adet interface kullanılacaktır.

**2.11.1.6.4** E-Posta sunucusu/sunucuları için güncel işletim sistemi kullanılacaktır.

**2.11.1.6.5** İşletim sistemi üzerinde performans ve güvenlik için uygun disk kapasiteleri belirlenecek ve konfigürasyonu yapılacaktır.

**2.11.1.6.6** Yüklenici, sistemin bileşenlerinin üreticisi tarafından yayınlanan kritik ve güvenlik yamalarını düzenli olarak sisteme geçecek, yama yönetimini yapacaktır.

**2.11.1.6.7** İhtiyaca göre oluşturulacak olan posta kutusu veri tabanı sayısı belirlenecek ve düzgün şekilde yapılandırılacaklardır.

**2.11.1.6.8** Oluşturulacak olan veri tabanları minimum kaynak kullanımı ile tüm sunucularda yedekli hale getirilecektir.

**2.11.1.6.9** Sunucuların down olması durumunda sistemin işleyişi ile ilgili test süreçleri yüklenici tarafından yapılacaktır.

**2.11.1.6.10** Veri Merkezi ile FKM arasındaki bağlantının gitmesi durumunda iki lokasyonun birbirinden habersiz olarak ayağa kalkması engellenecektir.

**2.11.1.6.11** Posta kutusu veri tabanı ve posta kutusu kota ayarlamaları yüklenici tarafından standarda uygun olarak gerçekleştirilmelidir.

**2.11.1.6.12** Kullanıcıların gönderebilecekleri ve alabilecekleri maksimum mesaj boyutu standarda uygun olarak gerçekleştirilmelidir.

**2.11.1.6.13** Gerektiği takdirde kullanıcıların mailing yapmasının engellenmesi için uygun tedbirler alınacaktır.

**2.11.1.6.14** Kullanıcıların maillerine erişimlerinde kullanılan protokollerin güvenliği sağlanacaktır.

**2.11.1.6.15** Sunucuların çok fazla log üretmesine karşı özellikle log diskleri düzenli olarak yedeklenecek ve temizlenecektir.

**2.11.1.7 Yedekleme Yazılımı;**

**2.11.1.7.1** Yedekleme yazılımı ilgili ürünün en iyi kurulum senaryosuna (Best Practice) göre gerçekleştirilecektir.

**2.11.1.7.2** Yedekleri saklamak için Windows, Linux, CIFS/SMB dosya paylaşımlarını ve üzerinde dahili tekilleştirme sunan cihazlar aktif edilecektir.

**2.11.1.7.3** Sanal sunucular ve üzerlerinde yer alan uygulamalar için uygun incremental ve full yedekleme görevleri oluşturulacaktır.

**2.11.1.7.4** Yedeklemelerin tutulacağı süre sunucunun kritiklik seviyesine ve yedekleme ünitesinin disk kapasitesine göre belirlenecektir.

**2.11.1.7.5** Yedekleme için oluşturulan görevlerde health-check özelliği devreye alınacaktır.

**2.11.1.7.6** Başarılı / Başarısız yedekler için alert notification bilgisi iletimi yapılandırılacaktır.

**2.11.1.7.7** Alınan yedeklerde encryption (şiftreleme) özelliği aktif edilecektir.

**2.11.1.7.8** Yedeklemelerde uygun sıkıştırma yöntemleri devreye alınacaktır.

**2.11.1.7.9** Yedeklemelerin ve restore işlemlerinin düzenli olarak test operasyonları yapılacaktır.

**2.11.1.7.10** Yedekleme işlemleri için gerekirse bir veya birden fazla Proxy sunucusu kullanımı yapılandırılacaktır.

### 2.11.2 Network Altyapısı Kurulum

**2.11.2.1** Yüklenici mevcut yapıdaki vlan'ları yeni switchlerde oluşturulacaktır.

**2.11.2.2** Mevcutta bulunan omurga switch ile yeni entegre olacak omurga switch arasında yedeklilik sağlanacak, bağlantılar kademe kademe taşınacaktır.

**2.11.2.3** Güvenlik duvarı ile yeni konumlandırılacak omurga switch arasındaki uplink'ler link-aggreation (LACP) moduna alınacaktır.

**2.11.2.4** Gerekli taşıma gerçekleştirildikten sonra (Kat Switchleri ve Sunucular) Mevcutta bulunan omurga switch devreden çıkartılacaktır.

**2.11.2.5** Yedekli çalışacak yeni omurga switchler arasında yedekllik kurulacaktır.

**2.11.2.6** Yedekli olarak çalışacak switchlere gelen ikinci yedek hatlar link-aggreation (LACP) yapılarak ikinci omurga switchte sonlandırılacak,

**2.11.2.7** Spanning tree'lerde root bridge olacak switch backbone üzerinde tanımlanacaktır,

**2.11.2.8** Yapıda kullanılacak herhangi Netflow, NAC vb. izleme ürünler için gerekli kısıtlamalar kaldırılıp iletişime açılacaktır.

### 2.11.3 Güvenlik Altyapısı Kurulum

**2.11.3.1 Firewall Kurulumları;**

**2.11.3.1.1** Güvenlik duvarı cihazlar A/P modda yedekli yapıda kurulacaktır

**2.11.3.1.2** Switch ile güvenlik duvarı arasında en az 2 adet 10Gbit port çapraz bağlantı yapılarak, LACP modda çalıştırılacaktır.

**2.11.3.1.3** Her birlik kendi güvenlik duvarını kendi kullanıcı adı ve parolası ile bağımsız olarak yönetebilecektir.

**2.11.3.2 SIEM Ürünü Kurulumu;**

**2.11.3.2.1** Tüm çalışan sistemlerden veri alacak şekilde ayarlanacaktır.

**2.11.3.2.2** Kuruma özel korelasyonlar teker teker kontrol edilecektir.

**2.11.3.2.3** SIEM ürünün yapılandırılması için minimum 10 adam/gün hizmet verilecektir.

**2.11.3.2.4** Mail Gateway Ürünü Kurulumu;

**2.11.3.2.5** Her birliğin kendi domain'ini kendi parolası ile yönetmesi sağlanacaktır.

**2.11.3.3 WAF Ürünü Kurulumu;**

**2.11.3.3.1** SSL sonlandırma WAF üzerinde yapılıp, load balance yapılacaktır.

**2.11.3.3.2** WAF ürünü önce monitör modda çalıştırılacak, verimli çalıştığı tespit edildikten sonra engelleme modunda çalıştırılacaktır.

**2.11.3.4** İhale kapsamında alınan diğer tüm güvenlik ürünleri yüklenici tarafından kurulup sağlıklı bir şekilde çalıştırılacaktır.

## 2.12 EĞİTİM

### 2.12.1 Eğitim Koşulları

**2.12.1.1** Yüklenici ihale kapsamında vereceği ürünler için kullanıcı eğitimi verecektir.

**2.12.1.2** Eğitimler TİM bünyesinde en fazla 5 kullanıcı için verilecektir.

**2.12.1.3** Eğitimler toplam 10 günde tamamlanacaktır.

**2.12.1.4** Eğitimler ürünlerin erişimi, temel kullanımı seviyesinde olacaktır.

### 2.12.2 Eğitim Verilecek Ürünlerin Listesi

**2.12.2.1** Sunucu eğitimi

**2.12.2.2** Depolama ürünleri eğitimi

**2.12.2.3** Ağ anahtarı ürünleri eğitimi

**2.12.2.4** Güvenlik duvarı ürünleri eğitimi

**2.12.2.5** Güvenlik bilgi ve olay yönetimi ürünü eğitimi

**2.12.2.6** E-posta Güvenliği ürünü eğitimi

**2.12.2.7** Web güvenliği ürünü eğitimi

**2.12.2.8** Sunucu güvenliği ürünü eğitimi

**2.12.2.9** Sanallaştırma ürünü eğitimi

**2.12.2.10** Yedekleme ürünü eğitimi

**2.12.2.11** E-posta sunucusu ürünü eğitimi

**2.12.2.12** İzleme ürünü eğitimi

**2.12.2.13** Veri Merkezi genel topolojisi bilgilendirme eğitimi

# 3 KISIM II – E-BİRLİK BULUT BİLİŞİM ve BARINDIRMA HİZMETLERİ

## 3.1 İŞİN KAPSAMI

İşbu şartnamenin bu bölümü KISIM I tamamlanana kadar (ve tamamlanmasa dahi) geçiş aşaması için yeni geliştirilen E-Birlik sistemi altyapısında kullanılacak donanım, yazılım, bilişim güvenliği ürünleri ve Veri Merkezi barındırma hizmetlerini tanımlamaktadır.

Bulut Bilişim Hizmetleri temel olarak, İDARE'ye ait fiziksel donanımların veri merkezinde barındırılması ve eksik her türlü sistem/network altyapı donanımlarının kiralanması ile birlikte ilgili Veri Merkezlerinde bakım-destek ve yönetilen hizmetlerin gerçekleştirilerek YÜKLENİCİ'nin bağlı olduğu internet omurgasının kullanılmasından ibarettir.

KISIM II, Temel olarak 4 ana mal ve hizmet kalemini içermektedir;

**I.** Donanım Taşınması ve Veri Merkezi Barındırma Hizmeti
**II.** Donanım Kiralama Hizmeti
**III.** İnternet Hizmeti
**IV.** Yönetilen Hizmetler (Bakım, Destek, Kurulum ve Eğitim)
**V.** Felaket Kurtarma Merkezi ve Yedekleme Hizmeti

Bulut Bilişim Hizmetleri kapsamında YÜKLENİCİ'nin verebileceği hizmetler EK-3'de detaylandırılmıştır.

## 3.2 GENEL HÜKÜMLER

**3.2.1.1** İhalenin sonuçlanmasına müteakip KISIM II için KISIM I'in tamamlanması ile sonlanacak (ya da KISIM I'in uzaması ihtimaline karşı 1 yıllık) bir sözleşme imzalanacaktır.

**3.2.1.2** İşbu ihaleyi kazanan YÜKLENİCİ, ilk etapta İDARE'nin E-Birlik tarafına ait 5 Adet sunucuyu KISIM II'ye ait sözleşmenin imzalanmasına müteakip çalışmalara başlayacak şekilde gerekli altyapıyı sağlayacak biçimde bir veri merkezinde barındıracaktır.

**3.2.1.3** EK-3'de yer alan konfigürasyon için birim fiyat üzerinden teklif verilecektir.

**3.2.1.4** İSTEKLİ, vereceği teklifte aylık hizmet bedellerini kalem bazında tekliflendirecektir.

**3.2.1.5** İDARE, KISIM II dahilindeki hizmeti kısmi alım olarak yapabilir. İzleme (Monitoring) Yazılımı, Çok Faktörlü Kimlik Doğrulama Yazılımı, Ayrıcalıklı Erişim Yönetimi (PAM) Ürünü, Web Zafiyet Tarama Yazılımı ya da donanım kiralamadaki Firewall vb. hizmet kalemlerini almayabilir.

**3.2.1.6** TARAFLAR, KISIM II sözleşmesi kapsamında 12 Ay boyunca sağlanacak Bulut Bilişim Hizmetlerinin ve bu Hizmetler karşılığında ödenecek, tüm vergiler hariç, aylık ve toplam tutarları kabul ve beyan edeceklerdir.

### 3.2.2 Hizmetler, Hizmet Bedeli Ve Ödeme Şartları

**3.2.2.1** Teknik şartnamede yer alan hizmet kalemleri için kalem birim fiyatları da içeren toplu teklif verilecektir.

**3.2.2.2** KISIM I'in tamamlanamaması halinde bir yıllık sözleşme süresince 6 ayda bir olmak koşuluyla birim fiyatlarda azami 6 aylık TÜİK'in açıklamış olduğu (TÜFE+ÜFE) /2 oranında artış yapılacak ve sözleşme süresi sonunda aynı artış oranı şartları ile yenilebilecektir.

**3.2.2.3** Tabloda belirtilen hizmetlerden sadece kullanılan hizmetler fatura edilecektir.

**3.2.2.4** Sözleşme birim fiyatlarının yenilenmesi zamanlarında Dolar olarak fiyatlandırılan kalemler için Amerika Birleşik Devletleri'nde açıklanan yıllık Tüketici Fiyat Endeksi (CPI) ve Üretici Fiyat Endeksi'nin (PPI) ortalaması oranında artış yapılacak ve sözleşme aynı şartlarla yenilecektir.

**3.2.2.5** YÜKLENİCİ, İDARE'ye her ay sonu mutabakat raporu sunacak, onay sonrası fatura kesecektir.

**3.2.2.6** İDARE'nin talebi doğrultusunda ileride kullanılacak (kiralanacak) ek kaynak artırımı fiyatlandırılmasında ilgili dönemdeki birim fiyatlar geçerli olacaktır. Tabloda birim fiyatı yazmayan ürünler için YÜKLENİCİ

fiyat çalışıp bilgi dönecek İDARE onayı sonrası artırıma gidilecek ve bir sonraki fatura dönemine yansıtılacaktır.

**3.2.2.7** İDARE tarafından kullanılan Microsoft CSP, Microsoft SPLA, Veeam, Zerto ve diğer benzeri aylık ödenen yazılım kiralama fiyatlarında İDARE tarafından ürün değişikliği talep edilmesi halinde, meydana gelebilecek fiyat farkları taraflar arasında imzalanacak ek protokollerle tespit edilecektir.

**3.2.2.8** YÜKLENİCİ tarafından ABD doları ($) cinsinden değerlenecek kalemler, fatura kesim tarihinde TCMB döviz alış kuru üzerinden dönüştürülüp TL olarak faturalandırılacaktır.

**3.2.2.9** YÜKLENİCİ EK-1: KISIM I- Ürün ve Hizmet Listesi'nde yer alan teklif edilecek ürünler ile ilgili her bir ticari kalem için ürün tesliminde ilgili kalemin %70'i, ürünlerin kurulumları sonrası yapılacak kabul tutanağı ile kalan %30'unu faturalandıracaktır. Kurulumlar tamamlandıktan sonra teklif edilen hizmetler içerisinde yer alan 60 aylık bakım süreci başlayacaktır. Bu ödeme planı dışında farklı bir ödeme opsiyonu olan adaylar teklif aşamasında bunu da takvimsel olarak belirtmelidir.

**3.2.2.10** YÜKLENİCİ EK-3: KISIM II- Hizmet Listesi'nde yer alan teklif edilecek hizmetler ile ilgili her bir ticari kalem için hizmet başlangıcında ilgili kalemin tamamı faturalandırılacaktır.

**3.2.2.11** Hizmet bedeline ilişkin faturalar, İDARE'nin belirteceği e-posta adreslerine elektronik ortamda iletilir. Fatura üzerinde açıklama alanına "TİM Bilgi Teknolojileri Şubesi" yazılmalıdır. Fiili hizmet başlangıç tarihinden itibaren sözleşme süresi boyunca fatura ödemelerini, fatura adresine ulaşmasına takiben 14 (ondört) iş günü içerisinde Fatura'da belirtilen hesap numaralarına gerçekleştirilir. Herhangi bir nedenle faturanın kendisine ulaşmadığı durumlarda İDARE, fatura ve ödeme bilgilerini YÜKLENİCİ'den öğrenebileceği gibi YÜKLENİCİ de İDARE'ye faturanın ulaşıp ulaşmadığını İDARE yetkilisinden teyit almakla yükümlüdür.

**3.2.2.12** İDARE, fatura edilen bedelin tamamını YÜKLENİCİ'nin sözleşme ya da fatura üzerinde belirtilen hesap numaralarından birine peşin, tam ve eksiksiz olarak ödeyeceğini taahhüt eder. İDARE'den kaynaklanan olası (öngörülemeyen, sehven), 10 iş gününü aşkın ödeme gecikmelerinde mutlaka telefon ile ilgili irtibat kişileri bilgilendirilmeli, ulaşılamama haber alınamama durumunda İDARE'nin mali işler şubesi ile irtibata geçilmelidir. İDARE'nin alacağı hizmetin üzerinde koşan yazılım Türkiye ihracatı için büyük önem arz eden, kamuyu ilgilendiren ihracatçıların üyelik ve gümrük beyanname süreçlerinin yönetildiği bir yazılımdır. Bu nedenle sadece resmi tebligat ve uyarılar sonrası İDARE'nin bilgisi ve onayı dahilinde hizmet kısıtlandırılabilir ya da sonlandırılabilir.

### 3.2.3 Yüklenicinin Genel Sorumlulukları

**3.2.3.1** YÜKLENİCİ proje kapsamında bir idari, bir de teknik "Müşteri Yetkilisi" (Account Manager) atayacaktır. Bu görevlilerin izne çıkışlarında (ya da raporlu olduklarında) yerlerine bakacak kişi(ler) İDARE'ye 1 hafta önceden bildirilecektir.

**3.2.3.2** İDARE, YÜKLENİCİ'den hizmetinden memnun olmadığı yetkililerin değişimini haklı sebeplere dayandırarak isteyebilir. Ortak karar sonrası değişimine karar verilirse gerekli aktarımların 10 iş günü içerisinde yapılması YÜKLENİCİ'nin yükümlülüğündedir.

**3.2.3.3** Özellikle teknik müşteri yetkilisi tüm çağrıların takibini yapmalı İDARE'yi farklı birim ya da yükleniciler ile muhatap olmak zorunda bırakmamalıdır.

**3.2.3.4** Yaşanılan sorunlar ve kesintiler sonrası YÜKLENİCİ müdahale süreleri içerisinde, muhteviyatında en az yaşanılan olayın anlatımı, kesinti süresi, tekrarını önlemek adına bir Düzenleyici Önleyici Faaliyet listesi olan "Vuku Raporu" hazırlayacaktır.

**3.2.3.5** Her ay sonu yapılacak mutabakat toplantıları kapsamında YÜKLENİCİ'nin yetkilendirdiği idari ve teknik müşteri yetkilileri ile birlikte İDARE yetkilileri ve İDARE'nin isteği doğrultusunda yetkilendirdiği ihracatçı birliklerin yetkililerinin katıldığı genel değerlendirme toplantısı yapılacaktır. Bu toplantılarda genel durum, kaynak kullanım eğilimleri (Trends), riskler, açılan biletler ve müdahale süreleri grafikler halinde sunulacak ve beraber değerlendirilecektir.

**3.2.3.6** YÜKLENİCİ, İDARE'nin kullanmakta olduğu kaynakları, bir online platform üzerinden izleyebilmesini sağlayacaktır. Söz konusu platform desteği YÜKLENİCİ tarafından sağlanamıyorsa dahi; Monitoring

hizmeti kapsamında YÜKLENİCİ tarafından kullanılmakta olan sistemde yetkilendirme yapılarak, İDARE envanterinin anlık/geriye dönük izlenebilmesi sağlanacaktır.

### 3.2.4 Tarafların Hak ve Yükümlülükleri

**3.2.4.1** YÜKLENİCİ, Bulut Bilişim Hizmetleri kapsamında hem İDARE'nin sunucularını hem de İDARE'ye hizmet kapsamında sunduğu donanım ve altyapı yazılımlarını YÜKLENİCİ Veri Merkezlerinde 7 gün 24 saat kesintisiz olarak muhafaza edilmesini ve İDARE'nin YÜKLENİCİ omurgasına bağlı olan bu donanımlara uzaktan erişim protokolleri aracılığı ile kontrolünü ve yönetimini sağlar.

**3.2.4.2** Uzaktan erişilemediği durumlarda İDARE'nin teknik yetkililerinin talimatları doğrultusunda YÜKLENİCİ uzmanları seviye I fiziksel müdahalelerde bulunacak yine sonuç alınamaz ise İDARE'nin teknik yetkililerinin fiziksel olarak donanımlara erişmesi için gerekli izinler de YÜKLENİCİ tarafından sağlanacaktır.

**3.2.4.3** TARAFLAR, KISIM II sözleşmesi ve eklerindeki yükümlülüklerin yanı sıra, mevcut ve ileride yürürlüğe girecek tüm ilgili yasalara, kanun ve mevzuata uygun davranmayı kabul ve taahhüt edecektir.

**3.2.4.4** YÜKLENİCİ, İDARE'nin verilerini muhafaza etmek ve güvenliğini sağlamakla yükümlüdür. YÜKLENİCİ'nin gerekli tedbirleri almaktaki eksikliği, kusuru ve benzeri nedenlerle meydana gelebilecek saldırılar ve/veya yetkisiz erişimler, İDARE'nin verilere erişiminde yaşayabileceği kesinti ve benzeri durumlardan YÜKLENİCİ sorumludur. Böyle bir ihlalin gerçekleşmesi halinde İDARE, derhal ve haklı nedenle sözleşmeyi feshedebilir. YÜKLENİCİ, İDARE'nin uğradığı zarar ve ziyanı tazmin ile yükümlüdür. YÜKLENİCİ tarafından muhafaza edilen sunucularda gelecek saldırılara ve bilgi hırsızlığına karşı İDARE, YÜKLENİCİ tarafından kurulan güvenlik sistemine riayet etmek ve gizliliği korumakla yükümlüdür. YÜKLENİCİ'nin aldığı önlemlere rağmen İDARE gereken özeni göstermez ve sisteminin kısmen veya tamamen zarar görmesine neden olursa bundan münhasıran İDARE sorumludur.

**3.2.4.5** YÜKLENİCİ'nin mülkiyetindeki donanımlar üzerindeki donanımsal arızaların giderilmesi, parça değiştirilmesi gibi gerekli tadilat, tamirat ve güncellemeler YÜKLENİCİ'nin sorumluluğundadır. Bu aşamalarda İDARE'ye sunulan hizmetlerde Hizmet Seviyesi taahhütleri kapsamında gerçekleşecek planlı kesintilerini, kesintinin önceden yazılı olarak bildirilmesi ve makul bir süreyle sınırlı olması kaydıyla İDARE onayına sunar, bu gibi durumlarda İDARE Türkiye ihracatının minimum etkileneceği saat dilimini seçme hakkına sahiptir. Bu durumlarda, gerekli işlemler YÜKLENİCİ tarafından Hizmet Seviyesi taahhütleri kapsamında tamamlanacak ve İDARE'nin bu durumdan etkilenmemesi ya da asgari seviyede etkilenmesi için gerekli önlemler YÜKLENİCİ tarafından alınacaktır.

**3.2.4.6** YÜKLENİCİ'nin, Sözleşme'ye aykırı davranması nedeniyle İDARE'nin uğrayacağı tüm zararlara karşı sorumluludur. Burada oluşacak anlaşmazlıkların (sözleşme aykırılığı tespiti, kusur tespiti, zarar tespiti vb.) çözümü için İstanbul Tahkim Merkezi yetkilidir.

### 3.2.5 Hizmet Seviyesi Taahhüdü (SLA)

**3.2.5.1** İşbu Hizmet Seviyesi Taahhüdü (SLA), KISIM II sözleşmesi kapsamında İDARE'ye sunulan veri merkezi hizmetlerinin kalite düzeyine ilişkin kuralları düzenlemektedir.

**3.2.5.2** İDARE'ye, KISIM II sözleşmesi kapsamında aldığı hizmetler için servis sağlanır.

**3.2.5.3** İDARE'nin KISIM II sözleşmesi kapsamında yer almayan ve/veya ek olarak aldığı diğer hizmet sağlayıcı firmalar üzerinden alınan hizmetler aşağıda taahhüt edilen Hizmet Seviyesi değerlerine dahil değildir. Hizmet Seviyesi taahhüdü sadece YÜKLENİCİ omurgası için geçerlidir.

**3.2.5.4** İDARE, Bulut Bilişim Hizmetleri ile ilgili oluşan problemlere ilişkin bildirimlerini arıza, şikâyet, değişiklik taleplerini, soru ve önerilerini sözleşmede belirtilen e-posta adresleri üzerinden ve YÜKLENİCİ'nin sunacağı çağrı (bilet) platformu üzerinden 7 gün 24 saat boyunca iletebilir.

**3.2.5.5** Hizmet Seviyesi taahhüdü, İDARE'nin ilgili e-posta adreslerine yapacağı bildirim (ya da çağrı platfomu üzerinden açtığı bilet) ile başlar. İDARE tarafından fark edilmeyen ve ilgili adreslere iletilmeyen sorunlardan ve bunların iletilmesine kadar geçen süreden YÜKLENİCİ sorumlu değildir. İDARE tarafından sorunun bildirilmesine kadar geçen süre, kesinti süresine dahil edilmez. Ancak

YÜKLENİCİ'nin izleme-destek hizmeti kapsamında fark ettiği arızi durumları YÜKLENİCİ vakit kaybetmeksizin İDARE'ye bildirecektir.

**3.2.5.6** YÜKLENİCİ planlı bakım çalışmalarını (acil ve/veya hızlı müdahale gerektiren durumlar planlı bakım olarak adlandırılmaz) en az 10 gün önce İDARE'ye onayına iletir. Bu gibi durumlarda İDARE Türkiye ihracatının minimum etkileneceği saat dilimini seçme hakkına sahiptir. Acil ve/veya hızlı müdahale gerektiren durumlarda YÜKLENİCİ mümkün olabildiğince İDARE'ye bilgilendirme yaparak bakımları gerçekleştirir.

**3.2.5.7** YÜKLENİCİ, Hizmet Seviyesi Taahhüdü kapsamındaki hizmetlerin İDARE'ye sağlanabilmesi için gerekli olan sistem ve ekipmanları IP (Internet Protokolü) adresi seviyesinde izler ve sorun anında İDARE'ye ulaşılabiliyorsa telefon ile, ulaşılamıyorsa e-posta yöntemiyle İDARE ile iletişime geçer ve İDARE, Hizmet Seviyesi Taahhüdü'ne göre gerekli müdahaleleri başlatır. YÜKLENİCİ, teknik olarak tespiti elverişli olmayan durumlarda sorunların proaktif tespit edilememesinden sorumlu değildir.

**3.2.5.8** Hizmet Seviyesi Taahhütleri, aksi belirtilmedikçe yıllıktır. SLA yıllık oran %99,98 dir.

**3.2.5.9** Soruna Müdahale ve Çözüm Zamanları:

| Şiddet Seviyesi | Tanım | Müdahale Süresi | Geçici Çözüm Süresi | Kalıcı Çözüm Süresi | Vuku Raporu Hazırlama |
|---|---|---|---|---|---|
| 1 (Kritik) | ➢ Sanal sunucu hizmetini sağlayan platformlarda oluşan arızalar nedeni ile, sistemlerin çalışmaması.<br>➢ Tüm Sanal uygulama ve veri tabanı sunucuların yanıt vermemesi, asılı (hang) konumda kalması, uzaktan bağlanılamaması<br>➢ Ağ (Network) erişiminin olmaması<br>➢ Disk erişiminden kaynaklı sorunlar | 15 Dk. | 30 Dakika | 4 saat | 2 Gün |
| 2 (Yüksek) | ➢ Sanal sunucu hizmetini sağlayan platformlarda oluşan arızalar nedeni ile, performans kayıpları<br>➢ Tüm Sanal uygulama ve veritabanı sunucularda performans kayıpları ve servislerin normalden yavaş çalışması<br>➢ Disk erişimi ile ilgili performans problemleri | 30 Dk. | 2 Saat | 8 Saat | 4 Gün |
| 3 (Orta) | ➢ Problemin müşterilere hizmet (iş) kaybına neden olmadığı durumlar. | 4 Saat | 24 Saat | 5 Gün | 1 Hafta |
| 4 (Düşük) | ➢ Müşteri Sistemlerinin direkt veya dolaylı olarak etkilenmediği ancak dış çevre faktörlerindeki kontrol edilemez riskleri barındıran sorunlar. | 8 Saat | 3 Gün | 1 Hafta | 1 Ay |

**3.2.5.10** Servis ve Erişebilirlik SLA Hesaplamaları aşağıdaki şekilde yapılacaktır ve yüzdelik değer üzerinden oransal olarak ifade edilecektir.

SLA = % ((Yıl Dakikaları – Arıza Süresi) / Yıl Dakikaları) *100)

İDARE'nin aldığı hizmetin 1(bir) yıldan kısa sürmesi durumunda SLA hesaplaması İDARE'nin kullandığı gün/dk üzerinden hesaplanır.

**Yıl Dakikaları:** Bir takvim yılı içerisinde dönem başlangıç günü ile dönem bitiş günü arasındaki toplam dakika süresidir. İDARE'nin YÜKLENİCİ Veri Merkezi Hizmetlerini almaya başladığı ilk takvim yılı için dönem başlangıç günü kontratın yürürlüğe girdiği gün, dönem bitiş günü 31 Aralık'tır. Diğer takvim yılları için dönem başlangıç günü 1 Ocak, dönem bitiş günü 31 Aralık'tır. Kontratın bittiği yıl için dönem başlangıç günü 1 Ocak, dönem bitiş tarihi kontratın son günüdür.

**Arıza Süresi:** Yukarıda belirtilen dönem başlangıç günü ile dönem bitiş tarihi arasındaki servis kesinti dakikalarıdır. Bu kesinti dakikalarına, aşağıda sayılan nedenlerden kaynaklanan kesintiler dahil değildir.

**3.2.5.11** Planlanmış periyodik bakım veya YÜKLENİCİ'nin üstlendiği onarımlar,

**3.2.5.12** İDARE veya fiili kullanıcı tarafından yapılan ihmalkâr davranış veya yanlış kullanımlar,

**3.2.5.13** İDARE sorumluluğundaki yazılımsal veya donanımsal tüm konfigürasyon tabanlı hatalardan kaynaklanan sorunlar,

**3.2.5.14** Bazı programlama ortamlarının güvenilirliği ile ilişkili kesintiler,

**3.2.5.15** Sunucu üzerindeki YÜKLENİCİ'nin kontrolü dışında çalışan servis, program veya uygulamalar,

**3.2.5.16** YÜKLENİCİ'nin kontrolü dışında ortaya çıkan nedenler,

**3.2.5.17** Aşağıda gösterilenler ile sınırlı olmaksızın mücbir sebepler:

a. Türk veya ilgili ülke resmi makamlarının, yükümlülüklerin yerine getirilmesini geciktiren veya bunları imkânsız kılan kararları, eylem veya işlemleri,
b. Deprem, savaş, abluka hali ile doğal afetler,

## 3.3 DONANIM TAŞINMASI VE VERİ MERKEZİ BARINDIRMA HİZMETİ

**3.3.1.1** İDARE'nin elinde E-Birlik'te kullanılmak üzere aşağıda detayları yer alan sunucular bulundurulmaktadır. Bu sunucuları İDARE'den alıp ilgili Veri Merkezlerine (Sunucu I, II, III Aktif DC, Sunucu IV, V Pasif DC) nakli ve kurulumu sonrası ayağa kaldırılması sağlanılacaktır;

**3.3.1.1.1** Sunucu I (Huawei RH 5885H v3)

**3.3.1.1.2** Sunucu II (Huawei RH 5885H v3)

**3.3.1.1.3** Sunucu III (Huawei RH 5885H v3)

**3.3.1.1.4** Sunucu IV (Huawei RH 5885H v3)

**3.3.1.1.5** Sunucu V (Huawei H88H v3)

## 3.4 DONANIM KİRALAMA HİZMETİ

**3.4.1.1** Bu sunucuların önüne Threat Protection Throughput (Tehdit Koruma) değeri en az 4 Gbps olan 2 adet yedekli şekilde konfigüre edilmiş Firewall konumlandırılacaktır.

## 3.5 VERİ MERKEZİ ERİŞİM HİZMETİ (İNTERNET)

**3.5.1.1** Bu sunucuların çalışabilmesi için /28 Subnet IP sağlanacaktır.

**3.5.1.2** E-Birlik sunucuları barındırma hizmeti kapsamında 1 Gbps bağlantı sağlanacaktır.

**3.5.1.3** KISIM I'in tamamlanması ile IP adresleri değişmeden KISIM I'e ait Ortak Veri Merkezine aktarılacaktır.

## 3.6 YÖNETİLEN HİZMETLER (BAKIM, DESTEK, KURULUM VE EĞİTİM)

### 3.6.1 Yönetilen Hizmetler Detaylar

**3.6.1.1** İşbu ihaleyi alan YÜKLENİCİ E-Birlik tarafına ait 5 Adet Sunucu için aşağıdaki hizmetleri/ürünleri sağlayacaktır.

**3.6.1.1.1** Proxmox kurulumu ve yapılandırması

**3.6.1.1.2** Proxmox'un HA yapıda kurulması

**3.6.1.1.3** Proxmox Backup Server kurulumu ve yapılandırması

**3.6.1.1.4** Load Balancer kurulumu ve yapılandırması

**3.6.1.1.5** WAF yapısının kurulumu ve yapılandırması

**3.6.1.1.6** YÜKLENİCİ, İşbu ihale KISIM I'de hangi marka WAF öneriyorsa o marka WAF konumlandıracaktır.

**3.6.1.1.7** 12 adet CPU için Proxmox Global İnternet sitesinde de yer alan **Proxmox Standard Support** sağlanması.

# EK-1: KISIM I- Ürün ve Hizmet Listesi

## Teklif edilecek ürünler

| No. | ÜRÜN ADI | BİRİM | MİKTAR |
|---|---|---|---|
| | Fiziksel Sunucu – Aktif DC | Adet | 5 |
| | Fiziksel Sunucu – Pasif DC | Adet | 2 |
| | Sunucu Depolama Ünitesi – Aktif DC | Adet | 1 |
| | Sunucu Depolama Ünitesi – Pasif DC | Adet | 1 |
| | SAN Switch – Aktif DC | Adet | 2 |
| | Veri Merkezi Ağ Anahtarı – Aktif DC | Adet | 2 |
| | Veri Merkezi Ağ Anahtarı – Pasif DC | Adet | 1 |
| | Yönetim Anahtarı – Aktif DC / Pasif DC | Adet | 3 |
| | Güvenlik Duvarı – Aktif DC | Adet | 2 |
| | Güvenlik Duvarı – Pasif DC | Adet | 2 |
| | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Adet | 1 |
| | E-posta Güvenliği Ürünü | Adet | 1 |
| | Web Güvenliği Ürünü | Adet | 1 |
| | Sunucu Güvenliği Ürünü | Adet | 1 |
| | Saldırı Yüzeyi Yönetimi Ürünü | Adet | 1 |
| | Sanallaştırma Yazılımı | Adet | 1 |
| | Yedekleme Yazılımı | Adet | 1 |
| | Sunucu İşletim Sistemi Ürünü | Adet | 1 |
| | Sunucu İşletim Sistemi Erişim Lisansı | Adet | 1 |
| | E-Posta Sunucusu | Adet | 1 |
| | E-Posta Sunucusu Erişim Lisansı | Adet | 1 |
| | Loglama ve Raporlama Ürünü | Adet | 1 |
| | İzleme (Monitoring) Yazılımı | Adet | 1 |
| | Çok Faktörlü Kimlik Doğrulama Yazılımı | Adet | 1 |
| | Ayrıcalıklı Erişim Yönetimi (PAM) Ürünü | Adet | 1 |
| | Web Zafiyet Tarama Yazılımı | Adet | 1 |

## Teklif edilecek hizmetler

| No. | ÜRÜN ADI | BİRİM | MİKTAR |
|---|---|---|---|
| | Operatör Hizmetleri | Ay | 60 |
| | Bakım Ve Yönetilen Hizmetler | Ay | 60 |
| | Yeni E-Birlik Sunucuları Barındırma | Ay | 60 |
| | Veri Merkezi Erişim Hizmeti (İnternet) | Ay | 1 |

# EK-2 KISIM I- Ürün ve Hizmet Listesi (Hyper-Converged Teklifi için)

## Teklif edilecek ürünler;

| No. | ÜRÜN ADI | BİRİM | MİKTAR |
|---|---|---|---|
| | Hiper Tümleşik (Hyper-converged Infrastructere) Altyapı – Aktif DC | Adet | 1 |
| | Hiper Tümleşik (Hyper-converged Infrastructere) Altyapı – Pasif DC | Adet | 1 |
| | Omurga Anahtar – Aktif DC / Pasif DC | Adet | 4 |
| | Yönetim Anahtarı – Aktif DC / Pasif DC | Adet | 4 |
| | NAS Depolama Ünitesi | Adet | 1 |
| | Güvenlik Duvarı – Aktif DC | Adet | 2 |
| | Güvenlik Duvarı – Pasif DC | Adet | 2 |
| | Güvenlik Bilgi ve Olay Yönetimi (SIEM) Ürünü | Adet | 1 |
| | E-posta Güvenliği Ürünü | Adet | 1 |
| | WEB Güvenliği Ürünü | Adet | 1 |
| | Sunucu Güvenliği Ürünü | Adet | 1 |
| | Sanallaştırma Ürünü – Aktif DC | Adet | 1 |
| | Sanallaştırma Ürünü – Pasif DC | Adet | 1 |
| | Yedekleme Yazılımı | Adet | 1 |
| | E-Posta Sunucusu Ürünü | Adet | 1 |
| | Sunucu İşletim Sistemi Ürünü – Aktif DC | Adet | 1 |
| | Sunucu İşletim Sistemi Ürünü – Pasif DC | Adet | 1 |
| | Zaman Damgası Çözümü | Adet | 1 |
| | İzleme Yazılımı | Adet | 1 |

## Teklif edilecek hizmetler

| No. | ÜRÜN ADI | BİRİM | MİKTAR |
|---|---|---|---|
| | Operatör Hizmetleri | Ay | 60 |
| | Bakım Hizmetleri | Ay | 60 |
| | Yeni E-Birlik Sunucuları Barındırma | Ay | 60 |
| | Veri Merkezi Erişim Hizmeti (İnternet) | Ay | 1 |

# EK-3: KISIM II- Hizmet Listesi

## Teklif edilecek hizmetler

| BULUT BİLİŞİM HİZMETİ | | | | | |
|---|---|---|---|---|---|
| **Kaynak** | **Bulut Hizmet açıklama** | **Adet** | **Birim** | **Birim Fiyat** | **Toplam** |
| | WAF | 4 | APP | | |
| | VERİ MERKEZİ ERİŞİM HİZMETİ (İnternet) | 1 | Gbps | | |
| | DDOS | 1 | Gbps | | |
| | PROXMOX SUPPORT HİZMETİ | 12 | CPU | | |
| | IP | 16 | Adet | | |
| | DESTEK HİZMETİ 7X24 | 5 | Sunucu | | |
| | LOAD BALANCER HİZMETİ | 4 | APP | | |
| | İDARE'nin sunucu I'i Barındırma | 1 | Adet | | |
| | İDARE'nin sunucu II'yi Barındırma | 1 | Adet | | |
| | İDARE'nin sunucu III'ü Barındırma | 1 | Adet | | |
| | İDARE'nin sunucu IV'ü Barındırma | 1 | Adet | | |
| | İDARE'nin sunucu V'i Barındırma | 1 | Adet | | |
| | Felaket Kurtarma Merkezi ve Yedekleme Hizmeti | 1 | Adet | | |
| **Toplam- Aylık (KDV Hariç)** | | | | | |