United Nations Development Programme

Empowered lives.
Resilient nations.

AMENDMENT NO. 6

Date: 15/06/2021

Subject : Amendment No:6 to Invitation to Bid (ITB) for "Procurement of Information Systems for Izmir Model Factory" within the scope of "Turkey Resilience Project in Response to the Syria Crisis, Component 1 – Job Creation" issued on 20 May 2021

Ref: UNDP-TUR-ITB(MC1)-2021/008

Dear Madam/Sir,

Please find **ATTACHMENT-1 Important Notes Regarding the Submission of Bids, ATTACHMENT-2 for "The revisions made to the ITB Clauses"** and **ATTACHMENT-3 Amended Version of Form E: Format of Technical Bid - SECTION 2: Scope of Supply, Technical Specifications, and Related Services** within the context of subject ITB issued on 20 May 2021 for "Procurement of Information Systems for Izmir Model Factory" within the scope of "Turkey Resilience Project in Response to the Syria Crisis, Component 1 – Job Creation".

You are kindly requested to prepare and submit your bids in response to our subject ITB with consideration of this amendment whereas all other clauses of the ITB remaining valid.

Please be informed that the deadline for submission of bids that was stated as June 15, 2021 07:00 a.m. – (New York local time Zone) has been extended to **June 23, 2021 07:00 am (EST/EDT New York Time)**.

Please be sure that your bids are submitted electronically on or before the submission deadline **June 23, 2021 07:00 a.m. – (New York local time Zone)** through e-tendering system**.**

ATTACHMENT-1 "Important Notes Regarding the Submission of Bids"

ATTACHMENT-2 "The revisions made to the ITB Clauses"

ATTACHMENT-3 "Amended Versions of Form E: Format of Technical Bid - SECTION 2: Scope of Supply, Technical Specifications, and Related Services"

Yours sincerely,

UNDP Turkey Country Office

ATTACHMENT-1 IMPORTANT NOTES REGARDING THE SUBMISSION OF BIDS

Bidders shall disregard the previous version of "Form E: Format of Technical Bid - SECTION 2: Scope of Supply, Technical Specifications, and Related Services" given in the Original ITB and prepare their bids as per the "Amended Version of Form E: Format of Technical Bid - SECTION 2: Scope of Supply, Technical Specifications, and Related Services" given as Attachment-3 in this Amendment. The bidders are also advised to take into consideration the amended version of Returnable Bid Forms published when preparing their bids.

ATTACHMENT-2 REVISIONS MADE TO THE ITB CLAUSES

With reference to Section 5a: Schedule of Requirements and Technical Specifications, and Form E: Format of Technical Bid under Section 6: Returnable Bidding Forms / Checklist; below clauses have been amended as follows:

Clause Nr.	***Clause in the Original ITB***	***Revised Clause***
"Section 5a: Schedule of Requirements and Technical Specifications" (pg.46) and "Section 6: Returnable Bidding Forms / Checklist, Form E: Format of Technical Bid, Section 2" (pg.126)	*6.7 The proposed processor architecture must be at least 64 bits, at least four cores must be at least 2.4 GHz.* *Teklif edilen işlemci mimarisi en az 64 bit, en az dört çekirdek en az 2.4 GHz olmalıdır.*	*6.7 The proposed processor architecture must be at least 64 bits, at least four cores must be at least 2.2 GHz.* *Teklif edilen işlemci mimarisi en az 64 bit, en az dört çekirdek en az 2.2 GHz olmalıdır.*
"Section 5a: Schedule of Requirements and Technical Specifications" (pg.47) and "Section 6: Returnable Bidding Forms / Checklist, Form E: Format of Technical Bid, Section 2" (pg.127)	*6.20 The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.* *Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.*	*This clause is removed from the ITB.*

ATTACHMENT-3 AMENDED VERSION OF FORM E: FORMAT OF TECHNICAL BID - SECTION 2: SCOPE OF SUPPLY, TECHNICAL SPECIFICATIONS, AND RELATED SERVICES

SECTION 2: Scope of Supply, Technical Specifications, and Related Services

This section should demonstrate the Bidder's responsiveness to the specification by identifying the specific components proposed, addressing the requirements, as specified, point by point; providing a detailed description of the essential performance characteristics proposed; and demonstrating how the proposed bid meets or exceeds the requirements/specifications. All important aspects should be addressed in sufficient detail.

IMPORTANT NOTE:

Bidders shall fill out below table in English by indicating the Brand Name and Model number of the products offered as well as the specifications of the offered products corresponding to the specifications listed in below table. If the offered product does not meet any of below minimum technical specifications, it will not be considered to be compliant and the offer will be disqualified. Please ensure that the offered product meets the minimum specifications requested below.

#	Item to be supplied description	*Tedarik edilecek ürün tanımı*	**Offered technical specifications by the Bidder shall be inserted in English** *Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir*
1. Server		*Sunucu*	**Brand/Model //** *Marka/Model:*
1.1	Each processor must support a 64-bit set of commands.	*Her bir işlemci 64-bit komut setini desteklemelidir.*	
1.2	There must be at least 2 physical processors on the server with an operating speed of at least 3.7 GHz.	*Sunucu üzerinde en az 2 adet, en az 3.7 GHz çalışma hızında fiziksel işlemci olmalıdır.*	
1.3	Each processor must have at least 8 cores. The server must have a total of at least 16 cores.	*Her bir işlemci en az 8 çekirdekli olmalıdır. Sunucuda toplam olarak en az 16 çekirdek olmalıdır.*	
1.4	Each processor must have at least 11 MB of cache.	*Her bir işlemci üzerinde en az 11 MB önbellek bulunmalıdır.*	
1.5	Each processor must have at least 2 UPI (Ultra Path Interconnect) connections.	*Her bir işlemci en az 2 adet UPI (Ultra Path Interconnect) bağlantı sayısına sahip olmalıdır.*	
1.6	Each memory used on the server will be PC4, DDR4.	*Sunucu üzerinde kullanılan her bir bellek PC4, DDR4 olacaktır.*	
1.7	There will be at least 384 GB of memory on the server. (each	*Sunucu üzerinde her biri 2666MT/s, en az 12 adet 32 GB*	

	2666MT/s and at least a capacity of 12*32 GB).	*kapasitesinde olan, toplamda en az 384 GB bellek bulunacaktır.*	
1.8	There will be at least 24 memory slots on the server.	*Sunucu üzerinde en az 24 adet bellek yuvası bulunacaktır*	
1.9	Memory modules will be ECC(Error Check Correction).	*Bellek modülleri ECC(Error Check Correction) özelliğinde olacaktır.*	
1.10	There should be a built-in dual SD card module on the server to be proposed.	*Teklif edilecek sunucu üzerinde dahili çift SD kart takılabilen modül bulunmalıdır*	
1.11	The server must have at least 2 microSDHC/SDXC cards with a capacity of 64 GB provided by the server manufacturer.	*Sunucu için en az 2 adet, sunucu üreticisinin sağladığı 64 GB kapasiteli, microSDHC/SDXC kart bulunmalıdır*	
1.12	Each server must have at least 1 interface to provide remote access and management at 10/100/1000Mbps.	*Her bir sunucu üzerinde en az 1 adet 10/100/1000Mbps hızında uzaktan erişim ve yönetim sağlayacak arabirimi olmalıdır.*	
1.13	Each server must have at least 4 1Gb Base-T and 2 10GB SFP+ Ethernet ports	*Her bir sunucu üzerinde en az 4 adet 1Gb Base-T ve 2 adet 10GB SFP+ ethernet bağlantı noktası bulunmalıdır*	
1.14	At least 2 SR SFP+ modules must be supplied with each server. SFP+ modules must be the original product. Equivalent products will not be accepted.	*Her bir sunucu ile birlikte en az 2 adet SR SFP+ modül verilmelidir. SFP+ modüller orijinal ürün olmalıdır. Muadil ürünler kabul edilmeyecektir*	
1.15	Each server must have at least 2 external HBA controllers running as 12Gbps SAS.	*Her bir sunucu üzerinde en az 2 adet 12Gbps SAS olarak çalışan harici HBA kontrol birimi bulunmalıdır.*	
1.16	The PDU and cables required for the server will be delivered together without previous use.	*Sunucu için gerekli PDU ve kablolar birlikte daha önce kullanılmamış olarak teslim edilecektir.*	
1.17	Each server must have at least 2 redundant power supplies, each with a power of 750W, which can be disassembled and installed during operation. At least 2 redundant power supplies, each with 2400W power, should be installed on the server if necessary.	*Her bir sunucu üzerinde çalışma esnasında sökülüp takılabilen; en az 2 adet, her biri 750W gücünde yedekli güç kaynağı bulunmalıdır. Sunucu üzerine gerektiğinde en az 2 adet, her biri 2400W gücünde yedekli güç kaynağı takılabilmelidir.*	
1.18	For each server, fans must be installed with at least 6	*Her bir sunucu için, çalışma esnasında sökülüp takılabilen*	

	redundant and all fan slots of the proposed system that can be disassembled and installed during operation.	*en az 6 adet yedekli ve teklif edilen sistemin tüm fan yuvaları dolu olacak şekilde fanlar takılı bulunmalıdır.*	
1.19	The server must support Trusted Platform Module 2.0 (TPM 2.0) and be offered with the necessary licenses	*Sunucuda Trusted Platform Module 2.0 (TPM 2.0) desteği bulunmalı ve gerekli lisanslar ile teklif edilmelidir*	
1.20	There must be at least 1 VGA port and 4 USB ports on the server to be offered.	*Teklif edilecek sunucu üzerinde en az 1 adet VGA portu, toplam 4 adet USB portu bulunmalıdır.*	
1.21	There must be at least 1 PCIe Gen3 x16 at least 4 PCIe slots on the server to be offered.	*Teklif edilecek sunucu üzerinde en az 1 adedi PCIe Gen3 x16 en az 4 adet PCIe slotu bulunmalıdır.*	
1.22	Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi operating systems may be installed on the servers.	*Sunucular üzerine, Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi işletim sistemleri kurulabilecektir.*	
1.23	The server to be offered must have a graphics card with at least 16mb of memory and supports a resolution of at least 1920*1200.	*Teklif edilecek sunucu üzerinde embedded olarak en az 16mb belleğe sahip ve en az 1920*1200 çözünürlüğü destekleyen grafik kartı bulunmalıdır.*	
1.24	At least 6 Single wide or at least 3 Double wide GPU cards can be installed on the server to be offered in necessary cases.	*Teklif edilecek sunucu üzerine gerektiğinde en az 6 adet Single wide veya gerektiğinde en az 3 adet Double wide GPU kart takılabilmelidir*	
1.25	The server must have a lockable front cover to prevent physical interference.	*Sunucu üzerinde fiziksel müdahaleleri engelleyebilmek için kilitlenebilir ön kapak bulunmalıdır.*	
1.26	The files required for system installation on the proposed server must be embedded and the system must be installed through the embedded system without the need for any disk drive.	*Teklif edilen sunucu üzerinde sistem kurulumu için gerekli dosyalar embedded olmalıdır ve herhangi bir disk, sürücü ye ihtiyaç olmadan embeded sistem üzerinden sistem kurulabilmelidir.*	
1.27	The server must have an LCD screen or warning lights showing system name, serial number, remote management IP number, power	*Sunucu üzerinde sistem ismi, seri numarası, uzaktan yönetim IP numarası, güç tüketimi ve arızaların kolay tespit edilebilmesini sağlayan*	

	consumption, and fault information that ensures easy detection of failures.	*arıza bilgilerini gösteren LCD ekran ya da uyarı ışıkları bulunmalıdır.*	
1.28	The server must have a remote management module with its own 1 Gb physical port that will provide access with HTTPS and SSLv2 certificates.	*Sunucu üzerinde HTTPS ve SSLv2 sertifika ile erişim sağlayacak kendine ait 1 Gb hızında fiziksel bağlantı noktasına sahip uzaktan yönetim modülü bulunmalıdır.*	
1.29	One of the USB ports on the front panel of the server must be accessible by the remote management port, a firmware update or authorization can be made with the USB memory that can be installed through this port when the server is closed, and the remote management web interface must be accessed by connecting it to a computer by USB cable when the remote management network is not installed or working.	*Sunucu ön panelinde bulunan USB portlardan bir adeti uzaktan yönetim portu tarafından erişilebilmeli, sunucu kapalı olduğu esnada bu port üzerinden takılabilecek USB bellek ile firmware güncellemesi veya provizyonlama yapılabilmeli ve uzaktan yönetim networkünün kurulu olmadığı veya çalışmadığı esnada USB kablo ile bir bilgisayara bağlayarak uzaktan yönetim web ara yüzüne erişilebilmelidir.*	
1.30	The remote management module must have HTML5 support and modern web servers should be managed without installing any agents, plugins, remote KVM access should be made, the operating system should be established by remote media connection and updates should be made.	*Uzaktan yönetim modülünün HTML5 desteği olmalı ve herhangi ajan, eklenti yüklenmeden modern web sunucuları yönetilmeli, uzaktan KVM erişimi yapılabilmeli, uzaktan medya bağlantısı yapılarak işletim sistemi kurulabilmeli ve güncellemeler yapılabilmelidir.*	
1.31	Servers must support virtual media, use USB sticks, CDs, DVDs, etc. connected to a remote computer.	*Sunucular sanal medya özelliğini desteklemelidir, uzaktaki bir bilgisayara bağlı USB bellek, CD, DVD, vb. medyaları kullanabilmelidir.*	
1.32	The remote management module should be able to manage the server RAID card, configure the disks to be added to the server later, and increase its capacity by adding disks to existing RAID groups.	*Uzaktan yönetim modülü sunucu RAID kartının yönetimini gerçekleştirebilmeli, sunucuya sonradan eklenecek disklerin RAID yapılandırmasını yapabilmeli ve mevcut RAID guruplarına disk eklemesi yaparak kapasitesini artırılmasını sağlayabilmelidir.*	

1.33	The server must be able to check the security and authenticity of the BIOS, firmware etc. files to be installed on it through the certificate, and there must be a secure non-volatile memory space on the server that ensures that security certificates are protected against attacks.	*Sunucu, üzerine yüklenecek BIOS, firmware vb dosyalarının sertifika vasıtası ile güvenliğini ve orijinalliğini kontrol edebilmeli, sunucu üzerinde, güvenlik sertifikalarının saldırılara karşı korunmasını sağlayan, uçucu olmayan güvenli bir bellek alanı bulunmalıdır.*	
1.34	There should be a metal alloy sliding rail system with accessories to prevent the proposed server from bending when pressed to ensure that it is pulled forward from the cab during operation.	*Teklif edilecek sunucunun çalışma esnasında kabinden öne çekilerek müdahale edilmesini sağlayacak üzerine baskı olduğunda eğilmesini engelleyecek aksesuarlara sahip metal alaşımlı kayan ray sistemi bulunmalıdır.*	
1.35	The server to be offered must have access and management support via mobile phone or tablet upon request.	*Teklif edilecek sunucunun istenildiğinde cep telefonu veya tablet üzerinden erişim ve yönetim desteği olmalıdır.*	
1.36	All components supplied with the server must be manufactured by the server manufacturer or approved by the server manufacturer and supplied by the server manufacturer and the current configuration of the server must be questioned through a portal belonging to the manufacturer, the server guarantee must cover all components on the server.	*Sunucu beraber verilen bütün komponentler sunucu üreticisi tarafından üretilmiş veya sunucu üreticisi tarafından onaylanarak tedariki sunucu üreticisi tarafından yapılmış olmalı ve üreticiye ait bir portal üzerinden sunucunun güncel konfigürasyonu sorgulanabilmeli, sunucu garantisi, sunucu üzerinde gelen bütün komponentleri kapsamalıdır.*	
1.37	It will operate on the city grid with 220 V AC and 50 Hz single or three-phase energy supply. Feed cable plugs for energy input will be of the appropriate type to the power distribution units in the existing cabinets.	*220 V AC ve 50 Hz tek veya üç faz enerji beslemesi ile şehir şebekesinde çalışacaktır. Enerji girişi için besleme kablo fişleri mevcut kabinler içerisindeki güç dağıtım ünitelerine uygun tipte olacaktır.*	
1.38	Servers will have a manufacturer's warranty on the next business day for at least 3 years. The letter that the warranty is given by the manufacturer should be provided in delivery time.	*Sunucular en az 3 yıl boyunca ertesi iş günü üretici garantisine sahip olacaktır. Garantinin üretici firma tarafından verildiğine dair yazı teslimat sırasında ibraz edilecektir.*	

Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
2. Data Storage Unit		***Veri Depolama ünitesi***	**Brand/Model //** ***Marka/Model:***
2.1	The data storage manufacturer to be offered will be the same brand or a brand of a soluiton partner as the proposed server computers.	*Teklif edilecek veri depolama üreticisi, teklif edilen sunucu bilgisayarlar ile aynı marka ya da çözüm ortağı firmanın markası olacaktır.*	
2.2	The external data storage system to be proposed must not consist of combining multiple data storage systems with clustering or similar methods.	*Teklif edilecek harici veri depolama sistemi, birden fazla veri depolama sisteminin kümeleme veya benzeri yöntemlerle birleştirilmesinden oluşmuş olmamalıdır.*	
2.3	Measures must be taken against a single-point error in the external data storage system to be offered and ensure that the backup unit data storage system operates continuously in case of failure of any part.	*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.*	
2.4	In case of any failure in the external data storage system to be proposed, the replacement of any part in the system (disc, power supply, fans, etc.) should be carried out without requiring system shutdown.	*Teklif edilecek harici veri depolama sisteminde herhangi bir sorun çıkması durumunda sistem içerisindeki herhangi bir parçanın (disk, güç kaynağı, fanlar, vs.) değiştirilmesi sistem herhangi bir sistem kapanması gerektirmeden yapılabilmelidir.*	
2.5	There must be two control units (dual controllers) on the external storage system.	*Harici depolama sistemi üzerinde iki adet kontrol ünitesi (dual controller) bulunmalıdır.*	

2.6	The proposed data storage unit must be able to connect the server with 16 Gb FC, 10 Gb SFP+ ISCSI, 10 Gb Base-T ISCSI, and 12 Gb SAS ports. At least 8 16 Gb FC, 10 Gb SFP+ ISCSI, 10 Gb Base-T ISCSI, and 12 Gb SAS ports should be installed on the proposed data storage unit as needed. In addition, the data storage unit must support at least 4 16Gb FC and at least 4 10Gb SFP+ ports on the device at the same time if desired (multi-protocol ports).	*Teklif edilen veri depolama ünitesi, 16 Gb FC, 10 Gb SFP+ ISCSI, 10 Gb Base-T ISCSI ve 12 Gb SAS portları ile sunucu bağlantısını sağlayabilmelidir. Teklif edilen veri depolama ünitesi üzerine ihtiyaca göre en az 8 adet 16 Gb FC, 10 Gb SFP+ ISCSI, 10 Gb Base-T ISCSI ve 12 Gb SAS portları takılabilmelidir. Ayrıca veri depolama ünitesi istenirse en az 4 adet 16Gb FC ve en az 4 adet 10Gb SFP+ portun aynı anda cihaz üzerinde bulunmasını desteklemelidir (multi-protocol ports).*	
2.7	Each controller will have a total of at least 8 pieces of 12 Gbps SAS ports, including at least 4 SAS ports at a speed of 12 Gbps.	*Her kontrol ünitesi (controller) üzerinde 12 Gbps hızında en az 4 adet SAS port olmak üzere toplamda en az 8 adet 12 Gbps SAS port bulunacaktır.*	
2.8	At least 2 pieces, at least 2 meters long, 12 Gbps, HD Mini-SAS to HD Mini-SAS cable will be supplied with the storage unit. All cables must belong to the storage manufacturer.	*Depolama ünitesi ile birlikte en az 2 adet, en az 2 metre uzunluğunda, 12 Gbps, HD Mini-SAS to HD Mini-SAS kablo verilecektir. Tüm kablolar depolama üreticisine ait olmalıdır.*	
2.9	Each control unit must have a management port with a speed of at least 1Gbps.	*Her kontrol ünitesi yönetim için en az 1Gbps hızına sahip yönetim portu bulunmalıdır.*	
2.10	Each controller on the external disk unit to be offered must have at least 8 GB of memory and a total of 16 GB of memory. This capacity must be dram type. Within the scope of this cache capacity, fields created with SSD/FMD, I/O card will not be accepted.	*Teklif edilecek harici disk ünitesi üzerinde bulunan her kontrol ünitesi üzerinde en az 8, toplamda ise 16 GB bellek bulunmalıdır. Bu kapasite DRAM tipinde olmalıdır. Bu önbellek kapasitesi kapsamında SSD/FMD, I/O kart ile oluşturulan alanlar kabul edilmeyecektir.*	
2.11	Firmware updates should be available without causing disruption to the running system.	*Çalışan sistem üzerinde kesinti yaratmadan firmware güncellemeleri yapılabilmelidir.*	
2.12	The Storage Unit should be able to expand to at least 276 disk capacity with the	*Depolama Ünitesi, teklif edilen kontrol birimleri ile en az 276 adet disk kapasitesine genişleyebilmeli ve en az 3PB*	

	proposed controllers and grow to at least 3PB capacity.	*kapasitesine kadar büyüyebilmelidir.*	
2.13	The system disk boost should be incremental in the form of racks and these racks should be manageable with an integrated HTML5 web-based GUI interface. Racks should be able to be created from 24 2.5" disks to provide the total number of discs, and the connection between the racks should be made with a 12 Gbit SAS interface. Each of the shelves should be no more than 2U high.	*Sistem disk artırımı raflar şeklinde arttırılabilir olmalı ve bu raflar entegre bir HTML5 web tabanlı GUI arayüzü ile yönetilebilir olmalıdır. Raflar toplam disk sayısını sağlamak üzere 24 adet 2.5" disklerden oluşturulabilmeli ve raflar arasındaki bağlantı 12 Gbit hızında SAS arayüz ile yapılmalıdır. Rafların her biri en fazla 2U yükseklikte olmalıdır.*	
2.14	The system must have at least 12 SSD drives with a connection speed of 12Gbps, ssd technology with a capacity of 960 GB, and SAS disks with a capacity of 1.8 TB with a rotational speed of at least 12 10000 RPM.	*Sistem üzerinde en az 12 adet, 12Gbps bağlantı hızında, 960 GB kapasiteli SSD teknolojisinde diskler ve en az 12 adet 10000 RPM dönüş hızında, 1.8 TB kapasiteli SAS diskler bulunmalıdır.*	
2.15	The disks used must be high-performance SAS, NL-SAS, SSD, and FIPS certified self-encrypting SAS and SSD in accordance with the selected disc racks.	*Kullanılan diskler seçilen disk raflarına uygun şekilde yüksek performanslı SAS, NL-SAS, SSD ve FIPS sertifikalı self-encrypting SAS ve SSD olabilmelidir.*	
2.16	The proposed data storage system must monitor the I/O that each disk makes, proactively monitor the health status performance graph, and work to provide the necessary warnings before the disk fails. Systems that fail to provide this must offer 30% additional capacity.	*Teklif edilen veri depolama sistemi her disk in yaptığı I/O yu izlemeli sağlık durumunu performans grafiğini proaktif olarak izlemeli ve disk bozulmadan önce gerekli uyarıları verecek şekilde çalışmalıdır. Bunu sağlayamayan sistemler %30 ilave kapasite verecek şekilde teklif etmelidirler.*	
2.17	The system must have Distributed RAID or similar technology that reduces rebuild times when disk failures occur on it.	*Sistem, üzerinde disk arızaları meydana geldiği zaman, yeniden oluşturma sürelerini azaltan Distributed RAID veya benzeri bir teknolojiye sahip olmalıdır.*	
2.18	The system should be able to support at least 64 host	*Sistem Fiber bağlantı seçeneği ile en az 64 adet host*	

	connections with a fiber connection option.	*bağlantısını destekleyebilmelidir.*	
2.19	The external disk system must support RAID levels 0, 1, 5, 6, and 10. Alternative data protection methods will not be accepted.	*Harici disk sistemi 0, 1, 5, 6 ve 10 RAID seviyelerini desteklemelidir. Alternatif veri koruma yöntemleri kabul edilmeyecektir.*	
2.20	Additions should be made to the virtual disk groups being used in the system without interruption of access.	*Sistemde kullanılmakta olan sanal disk gruplarına erişim kesintisi olmadan ilaveler yapılabilmelidir.*	
2.21	All licenses supported by the data storage unit (snapshot, clone, read cache, auto-tiering, replication, etc.) must be offered together with the proposed data storage unit in order to avoid additional costs at a later date.	*Teklif edilen veri depolama ünitesi ile birlikte ileri tarihlerde ek maliyet olmaması açısından, veri depolama ünitesinin desteklediği tüm lisanslar (snapshot, clone, read cache, auto tiering, replikasyon vb.) ile birlikte teklif edilmelidir.*	
2.22	The proposed data storage system should support the use of SSDs, which can be added to the system if desired, as a read-cache. SSD cache capacity can be raised up to 4TB. If there is an additional license requirement for this feature, it must be included in the offer.	*Teklif edilecek veri depolama sistemi, istendiği takdirde sisteme eklenebilecek SSD'lerin okuma amaçlı önbellek olarak kullanımını desteklemelidir. SSD önbellek kapasitesi 4TB'a kadar yükseltilebilmelidir. Bu özellik için ek bir lisans gereksinimi varsa teklife dahil edilmelidir.*	
2.23	The data storage system to be offered must have automatic data tiering that supports at least 3 layers (SSD, SAS, NL-SAS/SATA). By monitoring data activities on storage areas at the sub-LUN level, the data storage system should be able to automatically move heavily used sub-logical areas to faster storage and underused sub-logical areas to slower storage (automatic data tiering). Within the scope of this property, the data must be in the form of moving movements between layers, not in the form of copying. If	*Teklif edilecek veri depolama sistemi, en az 3 katmanı (SSD, SAS, NL-SAS/SATA) destekleyen otomatik veri katmanlandırma özelliğine sahip olmalıdır. Veri depolama sistemi, depolama alanları üzerindeki veri aktivitelerini alt mantıksal alan (sub-LUN – blok) seviyesinde izleyerek, yoğun kullanılan alt mantıksal alanları daha hızlı depolama alanına ve az kullanılan alt mantıksal alanları daha yavaş depolama alanına otomatik olarak taşıyabilmelidir (otomatik veri katmanlandırma). Bu özellik kapsamında verilerin*	

	a license is required to provide such a feature, the required licenses will be included in the offer for the maximum capacity supported by the system.	*katmanlar arasındaki hareketleri taşıma şeklinde olmalı, kopyalama şeklinde olmamalıdır. Sözkonusu özelliğin sağlanabilmesi için lisans gerekmesi durumunda, gerekli olan lisanslar, sistemin desteklediği maksimum kapasite için teklife dahil edilecektir.*	
2.24	The proposed data storage unit must support "thin provisioning".	*Teklif edilen veri depolama ünitesi "thin provisioning" desteği olmalıdır.*	
2.25	At least 512 (five hundredonics) LUNs must be created in the proposed data storage unit.	*Teklif edilen veri depolama ünitesinde en az 512 (beşyüzoniki) LUN yaratılabilmelidir.*	
2.26	The external data storage system to be offered must be able to receive snapshots and full copies (clones) and return them (restored). The licenses required for this feature will be added to the offer for the maximum capacity supported by the system.	*Teklif edilecek harici veri depolama sistemi snapshot (anlık kopya) ve tam kopya (clone) alabilmeli ve bu kopyalardan geri dönebilmelidir (restore). Bu özellik için gerekli lisanslar sistemin desteklediği maksimum kapasite için teklife eklenecektir.*	
2.27	The external data storage system to be offered should use the ROW (Redirect on Write) method and not the COW (Copy on Write) method to avoid affecting the snapshot. Working principles will be documented with manufacturer's documents.	*Teklif edilecek harici veri depolama sistemi anlık kopyalama (snapshot) perfomansın etkilenmemesi için ROW (Redirect on Write) metodunu kullanmalı, COW (Copy on Write) metodunu kullanmamalıdır. Çalışma prensipleri üretici dökümanları ile belgelenecektir.*	
2.28	The proposed data storage unit must support at least 1024 snapshots.	*Teklif edilen veri depolama ünitesinin en az 1024 adet snapshot desteği olmalıdır.*	
2.29	The external data storage system to be offered is asynchronous, it must support replication. If additional hardware and licenses are required for this feature, it must be added to the offer for maximum capacity.	*Teklif edilecek harici veri depolama sistemi asenkron, replikasyonu desteklemelidir. Bu özellik için ek donanım ve lisans gerekiyorsa teklife maksimum kapasite için eklenmelidir.*	

2.30	The proposed data storage unit must have at least 2 redundant power supply with a power of at least 580 Watts. 2 power cables must be supplied with the data storage unit.	*Teklif edilen veri depolama ünitesi en az 2 adet, en az 580 Watt gücünde yedekli güç kaynağına (redundant power supply) sahip olmalıdır. Veri depolama ünitesi ile birlikte 2 adet güç kablosu verilmelidir.*	
2.31	External disk unit must support at least Vmware 6.0, 6.5, and 6.7; Windows Server 2012, 2016,2019, RHEL 6.0, and 7.4 SLES 12.3 operating systems.	*Harici disk ünitesi en az Vmware 6.0, 6.5 ve 6.7; Windows Server 2012, 2016,2019, RHEL 6.0 ve7.4, SLES 12.3 işletim sistemlerini desteklemelidir.*	
2.32	The external disk volume must support VMware vSphere (ESXi), Microsoft Hyper-V, and vCenter SRM.	*Harici disk ünitesinin VMware vSphere (ESXi), Microsoft Hyper-V ve vCenter SRM desteği olmalıdır.*	
2.33	Data Storage system management should be web-based without the need to install additional software.	*Veri Depolama sisteminin yönetimi ek bir yazılım yüklemeye gerek kalmadan web tabanlı olarak yapılabilmelidir.*	
2.34	The external data storage system to be offered will have the ability to alert the system administrator by e-mail in case of a failure on it.	*Teklif edilecek harici veri depolama sistemi, üzerinde oluşan bir arıza durumunda sistem yöneticisini e-posta ile uyarma özelliğine sahip olacaktır.*	
2.35	The data storage unit should have a next-day guarantee of the manufacturer for at least 3 years.	*Veri depolama ünitesi en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
3. Virtualization Software		***Sanallaştırma Yazılımı***	**Brand/Model //** ***Marka/Model:***
3.1.	Virtualization software will be licensed for a total of 6 CPUs.	*Sanallaştırma yazılımı toplam 6 CPU için lisanslandırılacaktır.*	

3.2.	The proposed virtualization software must allow over-commitment of virtual machines to be created on the same physical server above existing system resources.	*Teklif edilen sanallaştırma yazılımı aynı fiziksel sunucu üzerinde oluşturulacak sanal makinaların mevcut sistem kaynaklarının üzerinde kaynak atanmasına (over-commitment) izin vermelidir.*	
3.3.	The proposed virtualization software must support SMP (Symetric Multi Processing). In the proposed system, 128 virtual CPUs should be assigned to each virtual machine at any time.	*Teklif edilen sanallaştırma yazılımı SMP (Symetric Multi Processing) desteği olmalıdır. Teklif edilen sistemde her bir sanal makinaya istenildiğinde 128 adet sanal CPU atanabilmelidir.*	
3.4.	With the proposed virtualization software, 1TB of virtual memory should be assigned to each virtual machine.	*Teklif edilen sanallaştırma yazılımı ile her bir sanal makinaya 1TB sanal bellek atanabilmelidir.*	
3.5.	The proposed virtualization software should be able to enlarge the virtual machine disk as it fills up, instead of retrieving the assigned disk space for each virtual machine directly from the disk pool. (Thin Provisioning)	*Teklif edilen sanallaştırma yazılımı gerektiğinde her bir sanal makine için atanan disk alanın doğrudan disk havuzundan almak yerine, sanal makine diski doldukça büyütebilmelidir. (Thin Provisioning)*	
3.6.	The proposed virtualization software guest operating system "GuestOS" must support current versions of Windows 8, Windows 10, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Centos, Redhat, Ubuntu, Solaris, SUSE Linux, Debian, Oracle Linux, MacOSX, FreeBSD operating systems.	*Teklif edilen sanallaştırma yazılımı misafir işletim sistemi "Guest OS" olarak, Windows 8, Windows 10 , Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Centos, Redhat, Ubuntu, Solaris, SUSE Linux, Debian, Oracle Linux , MacOSX, FreeBSD işletim sistemlerinin güncel versiyonlarını desteklemelidir.*	
3.7.	The proposed virtualization software must allow the file system containing the disks and virtual machines given to virtual machines to be	*Teklif edilen sanallaştırma yazılımı, sanal makinalara verilen disklerin ve sanal makinaların bulunduğu dosya*	

	enlarged while the system is running.	*sisteminin sistem çalışırken büyütülmesine izin vermelidir.*	
3.8.	The proposed virtualization software should enable the assignment of 62TB virtual disks to virtual machines.	*Teklif edilen sanallaştırma yazılımı sanal makinalara 62TB boyutunda sanal diskler atanmasına olanak sağlamalıdır.*	
3.9.	Proposed virtualization software must be able to manage 64TB of storage	*Teklif edilen sanallaştırma yazılımı 64TB boyutundaki depolama alanlarını yönetebilmelidir*	
3.10.	Support data storage technologies such as FC, iSCSI, and NFS and data storage units that work with these technologies with the proposed virtualization software.	*Teklif edilen sanallaştırma yazılımı ile FC, iSCSI ve NFS gibi veri depolama teknolojilerini ve bu teknolojilerle çalışan veri depolama ünitelerini desteklemelidir.*	
3.11.	With the proposed virtualization software, authorization should be made in the system, allowing certain operational persons to access the entire virtual system or part of the virtual system and carry out management operations.	*Teklif edilen sanallaştırma yazılımı ile sistemde yetkilendirme yapılabilmeli, belirli operasyonel kişilerin tüm sanal sisteme veya sanal sistemin bir kısmına erişmelerine ve yönetim operasyonlarını gerçekleştirebilmelerine imkan tanımalıdır.*	
3.12.	With the proposed virtualization software, system performance should be monitored instantly or retrospectively for parameters such as CPU, memory, disk, and network, and a report should be obtained.	*Teklif edilen sanallaştırma yazılımı ile sistem performansı CPU, memory, disk ve network gibi parametreler için anlık veya geçmişe doğru izlenebilmeli, rapor alınabilmelidir.*	
3.13.	The proposed virtualization software must include centralized management software that enables the management of all virtual servers from a single center.	*Teklif edilen sanallaştırma yazılımı tüm sanal sunucuların tek bir merkezden yönetimini sağlayan merkezi yönetim yazılımını içermelidir. (Merkezi*	

	(Will be offered with centralized management software licenses)	*yönetim yazılımı lisansları ile teklif edilecektir)*	
3.14.	The centralized management software that comes with the proposed virtualization software must be connected and managed from the web interface.	*Teklif edilen sanallaştırma yazılımı ile gelen merkezi yönetim yazılımı web arayüzünden bağlanıp yönetmeye olanak sağlamalıdır.*	
3.15.	The proposed virtualization software must allow VLAN assignment to virtual servers.	*Teklif edilen sanallaştırma yazılımı sanal sunuculara VLAN atanmasına izin vermelidir.*	
3.16.	The proposed virtualization software must allow a copy of the virtual servers to be made while they are open.	*Teklif edilen sanallaştırma yazılımı sanal sunucuların açıkken bir kopyasının çıkarılmasına izin vermelidir.*	
3.17.	The proposed virtualization software should be able to transfer running virtual machines to another server within the virtualization system without the need for shared disk space when needed and perform this process for multiple virtual machines at the same time.	*Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinaları ihtiyaç duyulduğunda paylaşımlı bir disk alanına ihtiyaç duymaksızın sanallaştırma sistemi içindeki başka bir sunucuya aktarabilmeli, bu işlemi aynı anda birden fazla sanal makina için gerçekleştirebilmelidir.*	
3.18.	There should be clustering service support in the form of automatic operation of virtual machines that shut down when there is an out-of-control stop on one of the servers defined in the proposed virtualization software. This service should be prioritized between virtual machines.	*Teklif edilen sanallaştırma yazılımı içerisinde tanımlı sunuculardan birisinde kontrol dışı bir durma olduğunda kapanan sanal makinaların sistemdeki diğer sunucular tarafından otomatik olarak çalıştırılması şeklinde kümeleme hizmeti desteği olmalıdır. Bu hizmet için sanal makinalar arasında önceliklendirme yapılabilmelidir.*	
3.19.	The proposed virtualization software should allow	*Teklif edilen sanallaştırma yazılımı belirlenen sanal*	

	designated virtual machines to replicate on virtualization servers in the same location or remote location.	*makinaların aynı lokasyondaki veya uzak bir lokasyondaki sanallaştırma sunucuları üzerine replikasyon yapmasına olanak tanımalıdır.*	
3.20.	The proposed virtualization software should be able to work integrated with third-party antivirus solutions and enable virus scanning on virtual machines using agency-independent architecture.	*Teklif edilen sanallaştırma yazılımı üçüncü parti antivirus çözümleri ile entegre çalışabilmeli ve ajansız mimari kullanarak sanal makinalar üzerinde virüs taraması yapılmasına olanak sağlamalıdır.*	
3.21.	The proposed virtualization software must support the addition of CPU, memory, disk, and network cards to running virtual machines.	*Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinalara CPU, memory, disk ve network kartı eklenmesini desteklemelidir.*	
3.22.	The proposed virtualization software should be able to ensure that the physical servers it operates for the selected virtual machines continue to operate from other physical servers without interruption in the event of an unplanned outage.	*Teklif edilen sanallaştırma yazılımı seçilen sanal makinalar için çalıştığı fiziksel sunucuların plansız bir kesinti yaşaması durumunda, kesintisiz olarak diğer fiziksel sunuculardan çalışmasına devam etmesini sağlayabilmelidir.*	
3.23.	Performance monitoring software should be able to monitor performance according to disk, memory, CPU, and network resources.	*Performans izleme yazılımı disk, bellek, cpu ve network kaynaklarına göre performans izlemesi yapabilmelidir.*	
3.24.	Performance monitoring software should be able to automatically make adaptive threshold definitions for resource usage by learning the system resource usage curve and be able to sound the alarm when resource usage rises below or above this lower threshold.	*Performans izleme yazılımı sistem kaynak kullanım eğrisini öğrenerek otomatik olarak kaynak kullanımı için adaptif eşik tanımlamaları yapabilmeli ve kaynak kullanımını bu alt eşiğin altına veya üst eşiğin üstüne çıktığında alarm verebilmelidir.*	

3.25.	Performance monitoring software should be able to detect incidents that may cause performance problems by associating alarms, errors, or warnings in the system with source usage graphs when necessary.	*Performans izleme yazılımı gerektiğinde sistemdeki alarm, hata veya uyarıları kaynak kullanım grafikleri ile ilişkilendirerek performans sorununa neden olabilecek olayları tespit edebilmelidir.*	
3.26.	Performance monitoring software must have its own database, not need a third-party database.	*Performans izleme yazılımı kendi veritabanına sahip olmalı, üçüncü parti bir veritabanına ihtiyaç duymamalıdır.*	
3.27.	Performance monitoring software should be able to monitor all virtual machines in the system to check whether the amounts of resources assigned to virtual machines are correct and to make improvements in this regard.	*Performans izleme yazılımı sistemdeki tüm sanal makinaları izleyerek sanal makinalara atanan kaynak miktarlarının doğru olup olmadığını kontrol edebilmeli, bu konuda iyileştirmeler yapabilmek için tavsiyelerde bulanabilmelidir.*	
3.28.	All software updates and security patches that will be issued for at least 3 years with licenses for the proposed solution must be installed, as well as 5 days and 9 hours of support for 3 years.	*Teklif edilen çözüme ait lisanslar ile birlikte en az 3 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 3 yıl boyunca 5 gün 9 saat destek hizmeti verilmelidir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
4. Backup Software		***Yedekleme Yazılımı***	**Brand/Model //** ***Marka/Model:***
4.1.	The software must be able to back up virtual machines	*Yazılım Microsoft Hyper-V ve Vmware vSphere*	

	running on the Microsoft Hyper-V and VMware vSphere virtualization platform to the application-consistent image-based disk.	*sanallaştırma platformunda çalışan sanal makinaların uygulama tutarlı imaj tabanlı diske yedeklemesini yapabilmelidir.*	
4.2.	The software's management console must be able to work on any physical or virtual, server, or personal computer with a 64-bit Microsoft Windows operating system.	*Yazılımın yönetim konsolu 64 bit bir Microsoft Windows işletim sistemine sahip herhangi bir fiziksel veya sanal, sunucu veya kişisel bilgisayar üzerinde çalışabilmelidir.*	
4.3.	The software must be licensed on the basis of the physical processor of the main servers running the virtual machines that are protected (backed up and/or replicated). There should be no licensing model based on the number of Virtual Machines, disk capacities, and application agents.	*Yazılımın lisanslaması korunmakta (yedeklenmekte ve/veya replike edilmekte) olan sanal makinaları çalıştıran ana sunucuların fiziksel işlemcisi bazında olmalıdır. Sanal Makina sayısı, disk kapasiteleri ve uygulama ajanlarına göre bir lisanslama modeli olmamalıdır.*	
4.4.	In order to improve the backup and replication performance of the Software, the number of structural components such as consoles, proxics, and storage areas should be increased without the need for an additional license.	*Yazılımın yedekleme ve replikasyon performansını arttırmak amacı ile konsol, proksi ve depolama alanları gibi yapısal bileşenlerinin sayısı ilave bir lisans gerektirmeden arttırılabilmelidir.*	
4.5.	The Software must be able to use Windows, Linux, CIFS/SMB file shares, and devices that offer singularization to store backed-up virtual machines.	*Yazılım, yedeklenen sanal makinaları saklamak için Windows, Linux, CIFS/SMB dosya paylaşımlarını ve tekilleştirme sunan cihazları kullanabilmelidir.*	

4.6.	The software must use the Changing Block Tracking (CBT) feature offered by hypervisors for incremental backups.	*Yazılım artımlı yedekler için hipervizörlerin sunduğu Değişen Blok Takibi (CBT) özelliğini kullanmalıdır.*	
4.7.	The Software must provide backup options over the Direct Data Storage network, over the Network, or through the Hypervisor I/O platform when reading backups from the source.	*Yazılım yedekleri kaynaktan okurken Doğrudan Veri Depolama ağı üzerinden, Ağ üzerinden veya Hipervizör I/O platformu üzerinden yedekleme seçenekleri sunmalıdır.*	
4.8.	The Software must provide internal command-line (PowerShell) Support.	*Yazılım dahili komut satırı (PowerShell) Desteği sunmalıdır.*	
4.9.	The software must provide a file management interface that will allow file transfer between the main server and other servers and computers.	*Yazılım ana sunucu ve diğer sunucu ve bilgisayarlar arasında dosya transferini sağlayacak bir dosya yönetim arayüzü sunmalıdır.*	
4.10.	The software must provide the ability to move virtual machines over the main server and disk areas. It should be able to do this using Vmware vMotion, Storage vMotion, and/or its own transport technology.	*Yazılım sanal makinaları ana sunucu ve disk alanları üzerinde taşıma özelliği sunmalıdır. Bu işlemi Vmware vMotion, Storage vMotion ve/veya kendi taşıma teknolojisini kullanarak yapabilmelidir.*	
4.11.	The Software must offer internal compression and singularization that can be customized or disabled by the user without the need for any agent installation.	*Yazılım herhangi bir ajan kurulumu gerektirmeden kullanıcı tarafından özelleştirilebilen veya devre dışı bırakılabilen dahili sıkıştırma ve tekilleştirme sunmalıdır.*	
4.12.	The Software should provide the option to receive fast incremental backups for only one Virtual Machine from a backup task with more	*Yazılım, içerisinde birden fazla Sanal Makina bulunan bir backup görevi içerisinden sadece bir Sanal Makina için hızlı artımlı yedek alabilme seçeneği sunmalıdır.*	

	than one Virtual Machine in it.		
4.13.	The software must offer a single full and subsequent 'continuously incremental' backup, eliminating the need for a periodic full backup.	*Yazılım tek bir tam ve sonrasında 'sürekli artımlı' yedekleme sunarak periyodik full yedek alma ihtiyacını ortadan kaldıracak sentetik tam yedekleme sunmalıdır.*	
4.14.	The Software must be able to automatically copy all backups taken to a disk space or backups of selected Virtual Servers from within for the purpose of copying the backup to a second disk space or for long-term archiving purposes.	*Yazılım bir disk alanına alınmış yedeklerin tamamını veya içerisinden seçilen Sanal Sunucuların yedeklerini ikinci bir disk alanına yedeğin kopyalanması veya uzun dönem arşivlenmesi amacı ile otomatik olarak kopyalayabilmelidir.*	
4.15.	The Software must be able to access backups taken to a disk space, files from Windowsor Linux servers to tape units, tape libraries, and Virtual Tape Libraries.	*Yazılım bir disk alanına alınmış yedekleri, Windows veya Linux sunucular içerisinden dosyaları teyp ünitelerine, teyp kütüphanelerine ve Sanal Teyp Kütüphanelerine arsivleyebilmelidir.*	
4.16.	The Software must be able to identify the Cloud disk service offered by a manufacturer-approved service provider as a backup store where backups will be stored and use this space to store backups or copies of backups.	*Yazılım üretici onaylı bir servis sağlayıcı tarafından sunulan Bulut disk hizmetini, yedeklerin saklanacağı bir yedek deposu olarak tanımlayabilmeli ve bu alanı yedekleri veya yedeklerin kopyalarını saklama amaçlı kullanabilmelidir.*	
4.17.	The software must be able to encrypt stored backups and network traffic end-to-end (when transferring, transferring, and storing) AES256bit.	*Yazılım saklanan yedekleri ve ağ trafiğini uçtan uca (kaynakta, aktarırken ve depolarken) AES256bit şifreleyebilmelidir.*	
4.18.	The Software should be able to fully back up Virtual	*Yazılım Vmware vCloud Director yapısı üzerinden Sanal*	

	Machine, vApp, and metadata directly through the Vmware vCloud Director structure and restore the same components to their original location or on a different vCloud Director structure.	*Makina, vApp ve metadata'ları doğrudan tam yedekleyebilmeli ve aynı bileşenleri orjinal yerlerine ya da farklı bir vCloud Director yapısı üzerine geri yükleyebilmelidir.*	
4.19.	The software must be able to perform application-consistent image-based replication of virtual machines running on the Microsoft Hyper-V and VMware vSphere virtualization platform.	*Yazılım Microsoft Hyper-V ve Vmware vSphere sanallaştırma platformunda çalışan sanal makinaların uygulama tutarlı imaj tabanlı replikasyonunu yapabilmelidir.*	
4.20.	The Software must be able to operate the Virtual Server replicated on a master server from the desired return point with predefined Virtual Network settings.	*Yazılım bir ana sunucu üzerine replike edilmiş Sanal Sunucuyu istenilen geri dönüş noktasından, önceden tanımlanmış Sanal Ağ ayarları ile çalışır duruma getirebilmelidir.*	
4.21.	The Software must be able to operate the Virtual Machine with the Microsoft Windows operating system replicated on a master server from the desired return point with predefined IP settings.	*Yazılım bir ana sunucu üzerine replike edilmiş Microsoft Windows işletim sistemine sahip Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış IP ayarları ile çalışır duruma getirebilmelidir.*	
4.22.	The software should be able to replicate from the received backups and create the replication fallback points from the backup files.	*Yazılım alınan yedeklerden replikasyon yapabilmeli, replikasyon geri dönüş noktalarını yedek dosyalarından oluşturabilmelidir.*	
4.23.	The software must provide Planned Transport to organize data center migration without data loss. Virtual Servers within	*Yazılım veri kaybı olmadan veri merkezi taşımasını organize edecek Planlı Taşıma özelliği sunmalıdır. Plan kapsamındaki Sanal Sunucular belirtilen*	

	the scope of the plan should be automatically closed in the specified order and the changes should be transferred and made operational in the new location.	*sıraya göre otomatik olarak kapatılmalı, değişiklikler aktarılarak yeni lokasyonda çalışır hale getirilmelidir.*	
4.24.	The software must be able to make a virtual machine operational without the need for additional copying or intervention directly from the full or incremental backup file on the disk.	*Yazılım bir sanal makinayı doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilmelidir.*	
4.25.	The software must be able to restore a virtual machine from its full or incremental backup file to its original location or on another master server.	*Yazılım bir sanal makinayı tam veya artımlı yedek dosyasından orjinal yerine veya başka bir ana sunucu üzerine geri yükleyebilmelidir.*	
4.26.	When restoring a virtual machine from backup, the software should offer quick recovery by simply transferring the changing blocks.	*Yazılım bir sanal makinayı yedekten geri yüklerken sadece değişen blokları aktararak hızlı kurtarma özelliği sunmalıdır.*	
4.27.	The software must be able to restore the files of a virtual machine on the main server.	*Yazılım bir sanal makinanın ana sunucu üzerindeki dosyalarını geri yükleyebilmelidir.*	
4.28.	The software must be able to independently restore the selected virtual disks of a virtual machine.	*Yazılım bir sanal makinanın seçilen sanal diskleri bağımsız olarak geri yükleyebilmelidir.*	
4.29.	The Software must be able to restore the Complete Virtual Machine, a file from within the virtual machine, Microsoft Exchange, Active Directory, SharePoint application elements, and Microsoft SQL Databases from within snapshots on	*Yazılım HP 3PAR StoreServ, HP StoreVirtual, HP StoreVirtual VSA ile NetApp Data ONTAP tabanlı NetApp FAS, NetApp FlexArray (V-Serisi), NetAppData ONTAP Edge ve IBM N Serisi Veri Depolama ünitelerinin üzerindeki Snapshot'ların içerisinden*	

	the HP 3PAR StoreServ, HP StoreVirtual VSA, and NetApp Data ONTAP-based NetApp FAS, NetApp FlexArray (V-Series), NetAppData ONTAP Edge, and IBM N Series Data Storage units.	*Komple Sanal Makinayı, Sanal makinanın içinden bir dosyayı, Microsoft Exchange, Active Directory, SharePoint uygulama öğelerini ve Microsoft SQL Veri tabanlarını geri yükleyebilmelidir.*	
4.30.	The Software Application must be able to create a second backup on top of NetApp Data ONTAP-based NetApp FAS, NetApp FlexArray (V-Series), NetAppData ONTAP Edge VSA, and IBM N Series Data Storage using consistent NetApp Hardware Snapshots.	*Yazılım Uygulama tutarlı NetApp Donanımsal Snapshot'larını kullanarak NetApp Data ONTAP tabanlı NetApp FAS, NetApp FlexArray (V-Serisi), NetAppData ONTAP Edge VSA ve IBM N Serisi Veri Depolama ünitelerinin üzerine ikinci bir yedek oluşturabilmelidir.*	
4.31.	The software must be able to export groups, users, and computer accounts from within Microsoft Active Directory backups in LDIFDE format.	*Yazılım Microsoft Active Directory yedekleri içerisinden grupları, kullanıcıları ve bilgisayar hesaplarını LDIFDE formatında dışarı aktarabilmelidir.*	
4.32.	The Software must provide the ability to quickly search, find, .msg, or export e-mail items, contacts, or notes, including those permanently deleted from Microsoft Exchange 2010 and 2013 server backups, as files or email attachments with the .pst extension.	*Yazılım Microsoft Exchange 2010 ve 2013 sunucu yedekleri içerisinden kalıcı olarak silinmiş olanlar dahil e-posta, takvim öğesi, kişi veya notları hızlıca arama, bulma, .msg veya .pst uzantılı dosya veya eposta eklentisi olarak dışa aktarma olanağı sunmalıdır.*	
4.33.	The Software Microsoft SharePoint 2010 and 2013 server backups must provide the ability to quickly search, find, file, or export items and content	*Yazılım Microsoft SharePoint 2010 ve 2013 sunucu yedekleri öğeleri ve içerikleri hızlıca arama, bulma, dosya veya eposta eklentisi olarak dışarı aktarma olanağı sunmalıdır.*	

	as a file or email attachments.		
4.34.	The software must be able to restore databases from microsoft sql server backups to the local database server	*Yazılım Microsoft SQL Sunucu yedekleri içerisinden veritabanlarını yerel veritabanı sunucusuna geri yükleyebilmelidir*	
4.35.	The software should be able to integrate into the vSphere Web Client, instant-speed backups should be started here, information such as the status of the backups, unprotected virtual machines should be accessible directly from within the web client.	*Yazılım vSphere Web Client'a entegre olabilmeli, anlık hızlı yedeklemeler buradan başlatılabilmeli, yedeklerin durumları, korunmayan sanal makinalar gibi bilgilere doğrudan web client içerisinden erişilebilmelidir.*	
4.36.	The Software should be able to import its configuration backup into defined disk space without any user intervention and be restored to include all settings and definitions.	*Yazılım kendi konfigurasyon yedeğini herhangi bir kullanıcı müdahalesi gerekmeden tanımlı disk alanına alabilmeli ve tüm ayarları ve tanımlamaları içerecek şekilde geri yüklenebilmelidir.*	
4.37.	The software must be licensed for the main server environment consisting of 4 physical processors in the environment.	*Yazılım ortamdaki 4 fiziksel işlemciden oluşan ana sunucu ortamı için lisanslanmalıdır. işlemci üzerindeki çekirdek (core) sayısı lisans sayısını etkilememelidir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
5. Server Software		***Sunucu Yazılımı***	**Brand/Model //** ***Marka/Model:***

5.1.	At least 80 core Windows Server 2019 Standard licenses or equivalent must be issued with the proposed servers.	*Teklif edilen sunucularla birlikte en az 80 core Windows Server 2019 Standart lisansı ya da eşdeğeri verilmelidir.*	
5.2.	At least 20 Windows Server 2019 Cal licenses or equivalent must be issued with the proposed servers.	*Teklif edilen sunucularla birlikte en az 20 adet Windows Server 2019 Cal lisansı ya da eşdeğeri verilmelidir.*	
5.3.	At least 2 SQL Server 2019 *Standard Edition* licenses or equivalent must be issued with the proposed servers	*Teklif edilen sunucularla birlikte en az 2 adet SQL Server 2019 Standard Edition lisansı ya da eşdeğeri verilmelidir*	
5.4.	At least 20 SQL Server 2019 Cal licenses or equivalent must be issued with the proposed servers.	*Teklif edilen sunucularla birlikte en az 20 adet SQL Server 2019 Cal lisansı ya da eşdeğeri verilmelidir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
6. Backup Unit		***Yedekleme Ünitesi***	**Brand/Model //** ***Marka/Model:***
6.1.	The product to be offered will be the storage unit NAS device that can be connected to the network.	*Teklif edilecek ürün ağa bağlanabilen depolama ünitesi NAS cihazı olacaktır.*	
6.2.	The data backup unit to be offered will be rack-type attachable to rack cabinets.	*Teklif edilecek veri yedekleme ünitesi raf tipinde rack kabinlerine takılabilir yapıda olacaktır.*	
6.3.	The proposed product must have at least 8 3.5" disc slots. With the addition	*Teklif edilen üründe en az 8 adet 3,5" disk yuvası bulunmalıdır. Disk çekmecesi*	

	of disc drawers, 20 3.5" disc slots should be able to be accessed.	*ilavesi ile 20 adet 3,5" disk yuvasına çıkabilmelidir.*	
6.4.	The proposed product must support 108TB disk capacity.	*Teklif edilen ürün 108TB disk kapasitesini desteklemelidir.*	
6.5.	With the proposed product, specially manufactured discs will be supplied for AT least 8 NAB capacity 7200 rpm return speed SATA or NL-SAS type NAS devices.	*Teklif edilen ürünle birlikte en az 8 adet en az 8 TB kapasiteli 7200 rpm dönüş hızında SATA veya NL-SAS tipinde NAS cihazları için özel üretilmiş diskler verilecektir.*	
6.6.	The system memory of the proposed product must be at least 2 GB of DDR3. With the addition of the memory module, it should be able to increase to 16 GB capacity.	*Teklif edilen ürünün sistem belleği en az 2 GB DDR3 olmalıdır. Bellek modülü ilavesi ile 16 GB kapasiteye çıkabilmelidir.*	
6.7.	The proposed processor architecture must be at least 64 bits, at least four cores must be at least 2.2 GHz.	*Teklif edilen işlemci mimarisi en az 64 bit, en az dört çekirdek en az 2.2 GHz olmalıdır.*	
6.8.	The proposed product must support 2.5" and 3.5" SATA and SSD discs.	*Teklif edilen ürün 2,5" ve 3,5" SATA ve SSD diskleri desteklemelidir.*	
6.9.	The proposed product must have at least 2 USB 3.0, at least 1 eSATA, and at least 4 Gigabit Ethernet ports supporting Link Aggregation and Failover.	*Teklif edilen ürün üzerinde en az 2 adet USB 3.0, en az 1 adet eSATA ve en az 4 adet Link Aggregation ve Failover destekleyen 1 Gigabit Ethernet portu bulunmalıdır.*	
6.10.	The proposed product must have at least 1 PCIe Expansion slot.	*Teklif edilen ürünün en az 1 adet PCIe Genişletme slotu bulunmalıdır.*	
6.11.	The product to be offered will have a power adapter with a power of at least 250W.	*Teklif edilecek olan ürünün en 250W gücünde güç adaptörü bulunacaktır.*	

6.12.	The device must be able to operate at temperatures from at least 5 °C to a maximum of 35 °C.	*Cihaz en az 5 °C ile en fazla 35 °C arasındaki sıcaklıklarda çalışabilmelidir.*	
6.13.	The warranty period of the device must be at least 3 years.	*Cihazın garanti süresi en az 3 yıl olmalıdır.*	
6.14.	The proposed product must support at least 512 folder shares.	*Teklif edilen ürün En az 512 adede kadar klasör paylaşımını desteklemelidir.*	
6.15.	The number of products iSCSI targets on offer must be at least 128 pieces.	*Teklif edilen ürün iSCSI hedef sayısı en az 128 adet olmalıdır.*	
6.16.	The number of iSCSI luns on offer must be at least 256 pieces.	*Teklif edilen ürün iSCSI lun sayısı en az 256 adet olmalıdır.*	
6.17.	The proposed product must support CIFS, AFP, NFS, FTP, WebDAV file protocols.	*Teklif edilen ürün CIFS,AFP,NFS,FTP,WebDAV dosya protokollerini desteklemelidir.*	
6.18.	The proposed product must support RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10 builds.	*Teklif edilen ürün RAID 0, RAID 1, RAID 5, RAID 6 ve RAID 10 yapılarını desteklemelidir.*	
6.19.	The proposed product must support at least 2048 local user accounts.	*Teklif edilen ürün en az 2048 adet yerel kullanıcı hesabını desteklemelidir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
7. Network Switch Type 1		***Ağ Anahtarı Tip 1***	**Brand/Model //** ***Marka/Model:***
7.1.	At least 4 1/10 GbE SFP/SFP+ slots must be	*Teklif edilen anahtar üzerinde maksimum konfigürasyonda*	

	supported in the maximum configuration on the proposed switch.	*en az 4 adet 1/10 GbE SFP/SFP+ yuva desteklenebilmelidir.*	
7.2.	At least 4 10G SR SFP+ Modules of the same brand as the manufacturer should be given with the proposed switch.	*Teklif edilen anahtar ile üretici ile aynı marka en az 4 adet 10G SR SFP+ Modül verilmelidir.*	
7.3.	The "Switching" capacity of the proposed switch must be at least 180 Gbps.	*Teklif edilen anahtarın "Switching" kapasitesi en az 180 Gbps olmalıdır.*	
7.4.	The "Forwarding" capacity of the proposed switch must be at least 130 million packets per second (Mpps).	*Teklif edilen anahtarın "Forwarding" kapasitesi en az 130 million packet per second (Mpps) olmalıdır.*	
7.5.	The proposed switch must have at least 48 Copper ports supporting the PoE+ standard at 10/100/1000.	*Teklif edilen anahtar üzerinde en az 48 adet 10/100/1000 hızında PoE+ standartını destekleyen Bakır port bulunmalıdır.*	
7.6.	The POE power budget of the proposed switch must be at least 370W.	*Teklif edilen anahtarın POE güç bütçesi en az 370W olmalıdır.*	
7.7.	The proposed switch must have 1 10/100 Mbps RJ-45 Ethernet Out of Band management port.	*Teklif edilen anahtar üzerinde 1 adet 10/100 Mbps RJ-45 Ethernet Out of Band management portu bulunmalıdır.*	
7.8.	The proposed switch must be in the stackable architecture. At least 8 devices must be supported in a stack.	*Teklif edilen anahtar yığınlanabilir mimaride olmalıdır. Bir yığın içerisinde en az 8 adet cihaz desteklenmelidir.*	
7.9.	The stacking bandwidth of the proposed switch must be at least 40 Gbps.	*Teklif edilen anahtarın yığınlama bant genişliği en az 40 Gbps olmalıdır.*	
7.10.	The proposed switch must be supplied with stacking modules if the cable required for stacking is required.	*Teklif edilen anahtar yığınlama için gerekli olan kablo gerekli ise yığınlama modülleri ile verilmelidir.*	

7.11.	The unit must be insertable and removable while the stack is running. For this purpose, at least one of the "Online Insertion/Removal" or "Hot Insertion/Removal" features should be supported.	*Yığın çalışır durumdayken ünite eklenebilir ve çıkarılabilir özellikte olmalıdır. Bu amaçla "Online Insertion/Removal" veya "Hot Insertion/Removal" özelliklerinden en az birisi desteklenmelidir.*	
7.12.	There must be at least 16,000 (sixteen thousand) MAC address support in the address table.	*Adres tablosunda en az 16.000 (onaltıbin) adet MAC adresi destegi olmalıdır.*	
7.13.	"MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" and " Per Vlan Rapid Spanning Tree + (PVST+)" must be supported on the proposed switch.	*Teklif edilen anahtar üzerinde "MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" ve " Per Vlan Rapid Spanning Tree + (PVST+)" desteklenmelidir.*	
7.14.	120 ports (Etherchannel/Link Aggregation Group/Trunk Group/Multi Trunk Link) must be created using the IEEE 802.3ad Link Aggregation protocol feature. At least 8 ports must be members of a "Link Aggregation Group".	*IEEE 802.3ad Link Aggregation protokolü özelliğini kullanarak 120 adet bağlantı noktası (Etherchannel/Link Aggregation Group/Trunk Group/Multi Link Trunk) oluşturulabilmelidir. Bir "Link Aggregation Group" `a en az 8 adet port üye olabilmelidir.*	
7.15.	At least 4000 (four thousand) VLAN configurations must be supported in the IEEE 802.1Q standard.	*IEEE 802.1Q standardında en az 4000 (dört bin) adet VLAN konfigürasyonu desteklenmelidir.*	
7.16.	At least one of the "RFC 3176 sFlow" or "Netflow" protocols must be supported in order to perform traffic analysis.	*Trafik analizi yapabilmek için "RFC 3176 sFlow" veya "Netflow" protokollerinden en az biri desteklenmelidir.*	
7.17.	Static routing, RIPv1/v2, and RIPng must be	*IPv4 ve IPv6 protokolleri için statik yönlendirme, RIPv1/v2 ve RIPng desteklenmelidir.*	

	supported for IPv4 and IPv6 protocols.		
7.18.	OSPF v2/v3 dynamic routing protocols must be supported by obtaining a license or software update on request.	*İstendiğinde lisans alınarak veya yazılım güncellemesi ile OSPF v2/v3 dinamik yönlendirme protokolleri desteklenebilmelidir.*	
7.19.	At least 1000 (thousand) directional registrations must be supported.	*En az 1000 (bin) adet yön kaydı desteklenmelidir.*	
7.20.	The "VRRP-E" or "HSRP" gateway must support at least one of the backup protocols by obtaining a license or software update on request.	*İstendiğinde lisans alınarak veya yazılım güncellemesi ile "VRRP-E" veya "HSRP" ağ geçidi yedekleme protokollerinden en az birini desteklemelidir.*	
7.21.	MLD snooping v1, v2 must be enabled so that IPv6 multicast traffic can be routed to the necessary interfaces and unnecessary multicast broadcasting can be blocked.	*IPv6 multicast trafiğinin gerekli arayüzlere yönlendirilebilmesi ve gereksiz multicast yayının engellenebilmesi için MLD snooping v1, v2 özelliği bulunmalıdır.*	
7.22.	PIM-SM (PIM Sparse Mode) and PIM-SSM (Source Specific Multicast) must be supported from dynamic multicast routing protocols with license or software updates on request.	*İstendiğinde lisans alınarak veya yazılım güncellemesi ile dinamik multicast yönlendirme protokollerinden PIM-SM (PIM Sparse Mode) ve PIM-SSM (Source Specific Multicast) desteklenmelidir.*	
7.23.	RADIUS and TACACS protocols and identification features should be supported.	*RADIUS ve TACACS protokolleri ile kimlik tanımlama özelliklerini desteklenmelidir.*	
7.24.	Access checklists must be supported.	*Erişim kontrol listeleri desteklenmelidir.*	
7.25.	At least one of the "Broadcast, multicast and unknown unicast rate-limiting" or "Storm	*"Broadcast, multicast and unknown unicast rate limiting" veya "Storm Control" özelliklerinden en az birisi desteklenmelidir.*	

	Control" features must be supported.		
7.26.	DHCP Relay, DHCP Server, and DHCP snooping features must be supported.	*DHCP Relay, DHCP Server ve DHCP snooping özelliklerini desteklenmelidir.*	
7.27.	The "Dynamic ARP Inspection" feature should be supported to protect against network attacks.	*Ağ ataklarına karşı koruma amaçlı "Dynamic ARP Inspection" özelliği desteklenmelidir.*	
7.28.	The "BPDU guard" feature must be supported to protect the "Spanning Tree" structure against external attacks.	*"Spanning Tree" yapısını dış ataklara karşı korumak için "BPDU guard" özelliği desteklenmelidir.*	
7.29.	The "Root Guard" feature must be supported to protect the selected switch from attacks and configuration errors.	*"Spanning Tree Root" seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı korumak için "Root Guard" özelliği desteklenmelidir.*	
7.30.	At least one of the "Multi-Device Authentication" or "Multidomain Authentication" features must be supported to support more than one 802.1x user per port at the same time.	*Port başına aynı anda birden fazla 802.1x kullanıcısının desteklenebilmesi adına "Multi Device Authentication" veya "Multidomain Authentication" özelliklerinden en az birisi desteklenmelidir.*	
7.31.	"VLAN Based Mirroring" or "VLAN ACL (VACL)" must be supported.	*"VLAN Based Mirroring" veya "VLAN ACL (VACL)" desteklenmelidir.*	
7.32.	Support for "Uni-Directional Link Detection (UDLD)" should be available to protect the health of connections between switching devices.	*Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı "Uni-Directional Link Detection (UDLD)" desteği bulunmalıdır.*	
7.33.	Cisco Discovery Protocol (CDP) or LLDP protocol must be supported to learn about neighboring devices.	*Komşu cihazları öğrenebilmek amacıyla Cisco Discovery Protocol (CDP) ya da LLDP protokolünü desteklenmelidir.*	

7.34.	Support for the "IEEE 802.1AB LLDP-MED" protocol must be available for automatic settings of edge devices such as IP Phones, such as QoS and VLAN.	*IP Telefon gibi uç cihazların QoS ve VLAN gibi ayarlarının otomatik olarak yapılabilmesi için "IEEE 802.1AB LLDP-MED" protokolü desteği bulunmalıdır.*	
7.35.	It must have support for marking the values "IEEE 802.1p" and "DSCP".	*"IEEE 802.1p" ve "DSCP" değerlerini işaretleme (marking/remarking) desteğine sahip olmalıdır.*	
7.36.	At least 8 priority/output queues (Priority/Egress Queue) must be defined.	*En az 8 adet öncelik/çıkış kuyruğu (Priority/Egress Queue) tanımlanabilmelidir.*	
7.37.	There must be support for applying speed restriction to traffic determined according to the access control list.	*Erişim kontrol listesine göre belirlenmiş bir trafiğe hız sınırlama uygulama desteği olmalıdır.*	
7.38.	The "SCP Secure Copy" protocol must be supported for secure file transfer purposes.	*Güvenli dosya transferi amacıyla "SCP Secure Copy" protokolü desteklenmelidir.*	
7.39.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	*Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
8. Network Switch Type 2 (NON-POE)		***Ağ Anahtarı Tip 2 (POE Olmayan)***	**Brand/Model //** ***Marka/Model:***
8.1.	At least 4 1/10 GbE SFP/SFP+ slots must be supported in the maximum	*Teklif edilen anahtar üzerinde maksimum konfigürasyonda en az 4 adet 1/10 GbE*	

	configuration on the proposed switch.	*SFP/SFP+ yuva desteklenebilmelidir.*	
8.2.	The "Switching" capacity of the proposed switch must be at least 180 Gbps.	*Teklif edilen anahtarın "Switching" kapasitesi en az 180 Gbps olmalıdır.*	
8.3.	The "Forwarding" capacity of the proposed switch must be at least 130 million packets per second (Mpps).	*Teklif edilen anahtarın "Forwarding" kapasitesi en az 130 million packet per second (Mpps) olmalıdır.*	
8.4.	There must be at least 48 10/100/1000 RJ45 Copper ports on the proposed key.	*Teklif edilen anahtar üzerinde en az 48 adet 10/100/1000 RJ45 Bakır port bulunmalıdır.*	
8.5.	The proposed switch must have 1 10/100 Mbps RJ-45 Ethernet Out of Band management port.	*Teklif edilen anahtar üzerinde 1 adet 10/100 Mbps RJ-45 Ethernet Out of Band management portu bulunmalıdır.*	
8.6.	The proposed switch must be in the stackable architecture. At least 8 devices must be supported in a stack.	*Teklif edilen anahtar yığınlanabilir mimaride olmalıdır. Bir yığın içerisinde en az 8 adet cihaz desteklenmelidir.*	
8.7.	The stacking bandwidth of the proposed switch must be at least 40 Gbps.	*Teklif edilen anahtarın yığınlama bant genişliği en az 40 Gbps olmalıdır.*	
8.8.	If the cable required for the proposed switch stacking is required, it must be supplied with stacking modules.	*Teklif edilen anahtar yığınlama için gerekli olan kablo gerekli ise yığınlama modülleri ile verilmelidir.*	
8.9.	The unit must be insertable and removable while the stack is running. For this purpose, at least one of the "Online Insertion/Removal" or "Hot Insertion/Removal" features should be supported.	*Yığın çalışır durumdayken ünite eklenebilir ve çıkarılabilir özellikte olmalıdır. Bu amaçla "Online Insertion/Removal" veya "Hot Insertion/Removal" özelliklerinden en az birisi desteklenmelidir.*	

8.10.	There must be at least 16,000 (hexadecimal) MAC address support in the address table.	*Adres tablosunda en az 16.000 (onaltıbin) adet MAC adresi destegi olmalıdır.*	
8.11.	"MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" and " Per Vlan Rapid Spanning Tree + (PVST+)" must be supported on the proposed switch.	*Teklif edilen anahtar üzerinde "MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" ve " Per Vlan Rapid Spanning Tree + (PVST+)" desteklenmelidir.*	
8.12.	120 ports (Etherchannel/Link Aggregation Group/Trunk Group/Multi Trunk Link) must be created using the IEEE 802.3ad Link Aggregation protocol feature. At least 8 ports must be members of a "Link Aggregation Group".	*IEEE 802.3ad Link Aggregation protokolü özelliğini kullanarak 120 adet bağlantı noktası (Etherchannel/Link Aggregation Group/Trunk Group/Multi Link Trunk) oluşturulabilmelidir. Bir "Link Aggregation Group" `a en az 8 adet port üye olabilmelidir.*	
8.13.	At least 4000 (four thousand) VLAN configurations must be supported in the IEEE 802.1Q standard.	*IEEE 802.1Q standardında en az 4000 (dört bin) adet VLAN konfigürasyonu desteklenmelidir.*	
8.14.	At least one of the "RFC 3176 sFlow" or "Netflow" protocols must be supported in order to perform traffic analysis.	*Trafik analizi yapabilmek için "RFC 3176 sFlow" veya "Netflow" protokollerinden en az biri desteklenmelidir.*	
8.15.	Static routing, RIPv1/v2, and RIPng must be supported for IPv4 and IPv6 protocols.	*IPv4 ve IPv6 protokolleri için statik yönlendirme, RIPv1/v2 ve RIPng desteklenmelidir.*	
8.16.	OSPF v2/v3 dynamic routing protocols must be supported by obtaining a license or software update on request.	*İstendiğinde lisans alınarak veya yazılım güncellemesi ile OSPF v2/v3 dinamik yönlendirme protokolleri desteklenebilmelidir.*	

8.17.	At least 1000 (thousand) directional registrations must be supported.	*En az 1000 (bin) adet yön kaydı desteklenmelidir.*	
8.18.	The "VRRP-E" or "HSRP" gateway must support at least one of the backup protocols by obtaining a license or updating software on request.	*İstendiğinde lisans alınarak veya yazılım güncellemesi ile "VRRP-E" veya "HSRP" ağ geçidi yedekleme protokollerinden en az birini desteklemelidir.*	
8.19.	PIM-SM (PIM Sparse Mode) and PIM-SSM (Source Specific Multicast) must be supported from dynamic multicast routing protocols with license or software update on request.	*İstendiğinde lisans alınarak veya yazılım güncellemesi ile dinamik multicast yönlendirme protokollerinden PIM-SM (PIM Sparse Mode) ve PIM-SSM (Source Specific Multicast) desteklenmelidir.*	
8.20.	MLD snooping v1, v2 must be enabled so that IPv6 multicast traffic can be routed to the necessary interfaces and unnecessary multicast broadcasting can be blocked.	*IPv6 multicast trafiğinin gerekli arayüzlere yönlendirilebilmesi ve gereksiz multicast yayının engellenebilmesi için MLD snooping v1, v2 özelliği bulunmalıdır.*	
8.21.	RADIUS and TACACS protocols and identification features should be supported.	*RADIUS ve TACACS protokolleri ile kimlik tanımlama özelliklerini desteklenmelidir.*	
8.22.	Access checklists must be supported.	*Erişim kontrol listeleri desteklenmelidir.*	
8.23.	At least one of the "Broadcast, multicast and unknown unicast rate limiting" or "Storm Control" features must be supported.	*"Broadcast, multicast and unknown unicast rate limiting" veya "Storm Control" özelliklerinden en az birisi desteklenmelidir.*	
8.24.	DHCP Relay, DHCP Server, and DHCP snooping features must be supported.	*DHCP Relay, DHCP Server ve DHCP snooping özelliklerini desteklenmelidir.*	
8.25.	The "Dynamic ARP Inspection" feature should	*Ağ ataklarına karşı koruma amaçlı "Dynamic ARP*	

	be supported to protect against network attacks.	*Inspection" özelliği desteklenmelidir.*	
8.26.	The "BPDU guard" feature must be supported to protect the "Spanning Tree" structure against external attacks.	*"Spanning Tree" yapısını dış ataklara karşı korumak için "BPDU guard" özelliği desteklenmelidir.*	
8.27.	The "Root Guard" feature must be supported to protect the selected key from attacks and configuration errors.	*"Spanning Tree Root" seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı korumak için "Root Guard" özelliği desteklenmelidir.*	
8.28.	At least one of the "Multi Device Authentication" or "Multidomain Authentication" features must be supported to support more than one 802.1x user per port at the same time.	*Port başına aynı anda birden fazla 802.1x kullanıcısının desteklenebilmesi adına "Multi Device Authentication" veya "Multidomain Authentication" özelliklerinden en az birisi desteklenmelidir.*	
8.29.	"VLAN Based Mirroring" or "VLAN ACL (VACL)" must be supported.	*"VLAN Based Mirroring" veya "VLAN ACL (VACL)" desteklenmelidir.*	
8.30.	Support for "Uni-Directional Link Detection (UDLD)" should be available to protect the health of connections between switching devices.	*Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı "Uni-Directional Link Detection (UDLD)" desteği bulunmalıdır.*	
8.31.	Cisco Discovery Protocol (CDP) must support CDP or LLDP protocol in order to learn about neighboring devices.	*Komşu cihazları öğrenebilmek amacıyla Cisco Discovery Protocol (CDP) ya da LLDP protokolünü desteklemelidir.*	
8.32.	Support for the "IEEE 802.1AB LLDP-MED" protocol must be available for automatic settings of edge devices such as IP Phones, such as QoS and VLAN.	*IP Telefon gibi uç cihazların QoS ve VLAN gibi ayarlarının otomatik olarak yapılabilmesi için "IEEE 802.1AB LLDP-MED" protokolü desteği bulunmalıdır.*	

8.33.	Must have support for marking the values "IEEE 802.1p" and "DSCP".	*"IEEE 802.1p" ve "DSCP" değerlerini işaretleme (marking/remarking) desteğine sahip olmalıdır.*	
8.34.	At least 8 priority/output queues (Priority/Egress Queue) must be defined.	*En az 8 adet öncelik/çıkış kuyruğu (Priority/Egress Queue) tanımlanabilmelidir.*	
8.35.	There must be support for applying speed restriction to traffic determined according to the access control list.	*Erişim kontrol listesine göre belirlenmiş bir trafiğe hız sınırlama uygulama desteği olmalıdır.*	
8.36.	The "SCP Secure Copy" protocol must be supported for secure file transfer purposes.	*Güvenli dosya transferi amacıyla "SCP Secure Copy" protokolü desteklenmelidir.*	
8.37.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	*Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
9. Wireless Access Point		***Kablosuz Erişim Noktası***	**Brand/Model //** ***Marka/Model:***
9.1.	It should be able to operate simultaneously in 2.4GHz and 5 GHz Frequency bands.	*2.4GHz ve 5 GHz Frekans bantlarında aynı anda çalışabilmelidir.*	
9.2.	12.2. IEEE must support 802.11b/g/a/n/ac wave 2 standards.	*IEEE 802.11b/g/a/n/ac wave 2 standartlarını desteklemelidir.*	
9.3.	12.3. 802.11n technology should support 20 MHz,	*802.11n teknolojisinde hem 2.4 GHz hem de 5 GHz*	

	and 40 Mhz signals in both 2.4 GHz and 5 GHz bands. 80 MHz signal should support 5 GHz signal in 802.11ac technology.	*bantlarında 20 MHz, ve 40 Mhz sinyalleri desteklemelidir. 802.11ac teknolojisinde 5 GHz bandında 80 MHz sinyali desteklemelidir.*	
9.4.	12.4. The following performance values must be supported: a) 802.11ac: 6.5 Mbps – 867 Mbps b) 802.11n: 6.5Mbps – 300 Mbps c) 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps d) 802.11b: 11, 5.5, 2, 1 Mbps	*Aşağıdaki performans değerleri desteklenmelidir:* *a) 802.11ac: 6.5 Mbps – 867 Mbps* *b) 802.11n: 6.5Mbps – 300 Mbps* *c) 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps* *d) 802.11b: 11, 5.5, 2, 1 Mbps*	
9.5.	Support Transmit BeamForming technology.	*Transmit BeamForming teknolojisini desteklemelidir.*	
9.6.	It must have intelligent antenna technology that can dynamically shape the broadcast area and provide advanced RF management by changing antenna coverage. 128 different broadcast areas must be dynamically created. In this way, an additional gain of 4 dB should be achieved in the direction of Transmit to antenna power. Thanks to the dynamically shaped broadcast area, signals should not be sent in directions where there is no communication, such broadcasts should be weakened at a rate of 10 dB.	*Dinamik olarak yayın alanını şekillendirebilen akıllı bir anten teknolojisine sahip olmalı ve anten kapsama alanlarını değiştirerek ileri düzey RF yönetimi sağlamalıdır. 128 farklı yayın alanı dinamik olarak yaratılabilmelidir. Bu sayede anten gücüne Transmit yönünde 4 dB ilave kazanç sağlanabilmelidir. Dinamik olarak şekillendirilebilen yayın alanı sayesinde haberleşmenin olmadığı yönlere sinyal gönderilmemeli, bu tür yayınlar 10 dB oranında zayıflatılmalıdır.*	
9.7.	Radio Frequency output power should be 23 dBm	*Radyo Frekansı çıkış gücü 2.4 GHz için 23 dBm, 5 GHz için 23 dBm olmalıdır.*	

	for 2.4 GHz and 23 dBm for 5 GHz.		
9.8.	Reception sensitivity must be up to -101 dBm.	*Alış hassasiyeti -101 dBm'e kadar olmalıdır.*	
9.9.	Must have at least 2x2 MIMO antenna structure.	*En az 2x2 MIMO anten yapısına sahip olmalıdır.*	
9.10.	At least 2 Spatial-Streams must be supported.	*En az 2 Spatial-Stream desteklenmelidir.*	
9.11.	Support 256 users at the same time.	*Aynı anda 256 kullanıcı desteklemelidir.*	
9.12.	The channel must be able to select automatically.	*Kanal seçimini otomatik yapabilmelidir.*	
9.13.	Background Scanning should allow you to detect interference (interference) in high-density environments and automatically select the appropriate channel by avoiding them.	*Background Scanning yaparak yüksek yoğunluklu ortamlardaki girişimleri (paraziti) tespit edebilme ve bunlardan sakınarak uygun kanalı otomatik olarak seçme özelliği bulunmalıdır.*	
9.14.	IP multicast video stream support must be available.	*IP multicast video stream desteği bulunmalıdır.*	
9.15.	IPv6 support must be available.	*IPv6 desteği bulunmalıdır.*	
9.16.	The device should be able to analyze packages automatically and assign them to the relevant queues using advanced service quality, packet classification, and automatic prioritization for latency-sensitive traffic.	*Cihaz paketleri otomatik olarak analiz edebilmeli, gecikmeye duyarlı trafik için ileri düzey servis kalitesi, paket sınıflandırma ve otomatik öncelik belirleme özelliklerini kullanarak bunları ilgili kuyruklara atayabilmelidir.*	
9.17.	There should be fair airtime fairness support.	*Adil yayın zamanı kullanım desteği (Airtime Fairness) olmalıdır.*	
9.18.	It should have the ability to automatically detect the highest performance channel and adjust itself to	*En yüksek performanslı kanalı otomatik olarak tespit edip kendisini o kanala ayarlama özelliği olmalıdır. En yüksek*	

	it. It should not interrupt communication with computers when scanning all channels for the purpose of detecting the highest performance channel.	*performanslı kanalı tespit amacıyla tüm kanalları tararken bilgisayarlarla olan iletişimi kesmemelidir.*	
9.19.	It should have VLAN support.	*VLAN desteği olmalıdır.*	
9.20.	WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i must support security features.	*WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i güvenlik özelliklerini desteklemelidir.*	
9.21.	Support port-based 802.1x security features over RADIUS (both authenticator and supplicant).	*Port tabanlı 802.1x güvenlik özelliklerini RADIUS üzerinden desteklemelidir (hem authenticator hem de supplicant olarak).*	
9.22.	It should have BandSteering capability and be able to force both 2.4 GHz and 5 GHz supported computers to connect over 5 GHz for load sharing when necessary.	*BandSteering özelliği olmalı ve gerekli gördüğünde yük paylaşımı için hem 2.4 GHz hem de 5 GHz destekli bilgisayarları öncelikle 5 GHz üzerinden bağlanmaya zorlayabilmelidir.*	
9.23.	16 BSSIDs should be supported where security and service quality policies can be set separately.	*Güvenlik ve servis kalitesi politikalarının ayrı ayrı ayarlanabileceği 16 adet BSSID desteklenmelidir.*	
9.24.	Support router feature including NAT and DHCP services.	*NAT ve DHCP servislerini de içeren router özelliğini desteklemelidir.*	
9.25.	HotSpot WLAN must dynamically have a user-by-user speed restriction feature.	*HotSpot WLAN için dinamik olarak kullanıcı bazında hız kısıtlama özelliği olmalıdır.*	
9.26.	It must be configured independently from the command line (Telnet/SSH), web interface (http/s), via Controller switch, via SNMP v1,2,3	*Bağımsız olarak komut satırından (Telnet/SSH), Web ara-yüzünden (http/s), Controller switch üzerinden, SNMP v1,2,3 yazılımı üzerinden konfigürasyonu*	

	software. Must support TR-069.	*yapılabilmelidir. TR-069 desteği olmalıdır.*	
9.27.	Be able to make software updates with FTP and TFTP.	*FTP ve TFTP ile yazılım güncellemeleri yapabilmelidir.*	
9.28.	It must be able to operate independently or in a controller control.	*Bağımsız olarak veya bir controller denetiminde çalışabilmelidir.*	
9.29.	When working independently, L2TP must be able to tunnel between it and the head office.	*Bağımsız olarak çalışırken merkez ofisle arasında L2TP tünel oluşturabilmelidir.*	
9.30.	When used with the controller it must support the following features: a) Authentication must be performed through the local database on the controller, via Active Directory, LDAP, or RADIUS server. b) Access control and load sharing between AP devices. c) Captive Portal and Guest user accounts that can authenticate over the web should be supported. d) In order to be able to roam quickly in voip and 802.1x EAP related applications, a tunnel must be established between the controller and the AP.	*Controller ile birlikte kullanıldığında aşağıdaki özellikleri desteklemelidir:* *i. Kimlik doğrulama işlemleri controller üzerindeki yerel veri tabanı üzerinden, Active Directory, LDAP veya RADIUS server üzerinden yapabilmelidir.* *ii. Erişim kontrolü ve AP cihazları arasında yük paylaşımı olmalıdır.* *iii. Web üzerinden kimlik doğrulaması yapabilen Captive Portal ve Misafir kullanıcı hesapları desteklenmelidir.* *iv. VoIP ve 802.1x EAP ile ilgili uygulamalarda hızlı roaming yapabilmek için controller ile AP arasında tünel oluşturulabilmelidir.*	
9.31.	Must have the following physical characteristics: a) Be able to feed on 12 VDC or PoE. If the DC adapter is received, it must	*Aşağıdaki fiziki özelliklere sahip olmalıdır:* *a) 12 VDC ile veya PoE üzerinden*	

	be able to operate between 110-240 VAC. b) Power consumption should be no more than 13W. c) It should be able to operate between 0°C and +40°C. d) Be able to work in relative humidity environments up to 95%. e) Kensington lock against theft should be possible. f) It must have a locking mechanism that will prevent accidental exit/fall from where it is installed. g) There must be one 10/100/1000BaseT Gigabit Ethernet port on it and it must be able to receive electricity via PoE. This port auto MDX should support auto-sensing. h) PoE power requirement must be within 802.3af standards. i) Energy saving feature.	*beslenebilmelidir. DC adaptör alınmışsa 110-240 VAC arasında çalışabilmelidir.* *b) Güç tüketimi en fazla 13W olmalıdır.* *c) 0°C ile +40°C arasında çalışabilmelidir.* *d) %95'e kadar bağıl nem ortamlarında çalışabilmelidir.* *e) Çalınmaya karşı Kensington kilit imkânı olmalıdır.* *f) Monte edildiği yerden kazara çıkmayı/düşmeyi engelleyecek bir kilit mekanizmasına sahip olmalıdır.* *g) Üzerinde bir adet 10/100/1000BaseT Gigabit Ethernet port olmalıdır ve bu port PoE üzerinden elektrik alabilmelidir. Bu port auto MDX, auto-sensing özelliğini desteklemelidir.* *h) PoE güç ihtiyacı 802.3af standartları içinde olmalıdır.* *i) Enerji tasarruf özelliği olmalıdır.*	

9.32.	Limited lifelong guarantee should be provided against manufacturing and labor defects.	*İmalat ve işçilik hatalarına karşı kısıtlı ömür boyu garanti sağlanmalıdır.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
10. Authentication and Network Access Control Software		***Kimlik Doğrulama ve Ağ Erişim Kontrol Yazılımı***	**Brand/Model //** ***Marka/Model:***
10.1.	The authentication and network access control platform can be offered to run on VMware infrastructure or as hardware.	*Kimlik doğrulama ve ağ erişim kontrol platformu, Vmware altyapısı üzerinde çalışacak şekilde veya donanım olarak teklif edilebilir.*	
10.2.	The authentication and network access control platform must work in full compatibility with the proposed network switches and wireless access devices.	*Kimlik doğrulama ve ağ erişim kontrol platformu, teklif edilen ağ anahtarları ve kablosuz erişim cihazları ile tam uyumlu çalışmalıdır.*	
10.3.	Authentication and network access control platform should not compromise system security, Vlan assignment, profiling, etc. In order to use its features, it should not request SNMP write right.	*Kimlik doğrulama ve ağ erişim kontrol platformu, sistem güvenliğini tehlikeye düşürmemeli, Vlan ataması, profillendirme vb. özelliklerin kullanılabilmesi amacıyla SNMP yazma (SNMP write) hakkı istememelidir.*	
10.4.	Authentication and network access control platform should work using	*Kimlik doğrulama ve ağ erişim kontrol platformu, IEEE 802.1x protokolünü kullanarak çalışmalıdır*	

	IEEE 802.1x protocol		
10.5.	The authentication and network access control platform should be able to work centrally. No additional hardware or software should be installed in the zones.	*Kimlik doğrulama ve ağ erişim kontrol platformu merkezi olarak çalışabilmelidir. Bölgelere ayrıca donanım veya yazılım kurulması gerekmemelidir.*	
10.6.	The authentication and network access control platform should be available for both wired and wireless network and VPN.	*Kimlik doğrulama ve ağ erişim kontrol platformu hem kablolu hem kablosuz ağ hem de VPN için kullanılabilmelidir.*	
10.7.	Authentication and network access control platform should work with RADIUS protocol.	*Kimlik doğrulama ve ağ erişim kontrol platformu RADIUS protokolü ile çalışmalıdır.*	
10.8.	Authentication and network access control platform should be managed through a single management screen.	*Kimlik doğrulama ve ağ erişim kontrol platformu tek bir yönetim ekranı üzerinden yönetilmelidir.*	
10.9.	Authentication and network access control platform for the network , including the last, which users / devices identity, group, device make and model, contact tour (wireless is) physically being connected location , post, applications running on running malicious software, if any, etc. must be able to see / learn information and take action accordingly.	*Kimlik doğrulama ve ağ erişim kontrol platformu Ağa dahil olan son kullanıcı/cihazların kimlik, grup, cihaz marka ve modeli, bağlantı turu, (kablosuz ise) bağlandığı fiziksel lokasyon, postur, üzerinde çalışan uygulama, varsa üzerinde çalışan zararlı yazılımlar vs. bilgileri görebilmeli/öğrenebilmeli ve bunlara göre aksiyon alabilmelidir.*	
10.10.	Authentication and network access control	*Kimlik doğrulama ve ağ erişim kontrol platformu NAC görevi*	

	platform should be able to act as NAC, it should be able to determine the current status of the operating system and antivirus application on the client, USB connection, disk encryption, etc. should be able to control.	*yapabilmeli, istemci üzerindeki işletim sistemi ve anti virüs uygulamasının güncellik durumlarını, USB bağlantısını, disk kriptosunu vs. kontrol edebilmelidir.*	
10.11.	The authentication and network access control platform must be licensed for at least 500 endpoints . The duration of the offered licenses must be at least 5 years.	*Kimlik doğrulama ve ağ erişim kontrol platformu en az 500 endpoint için lisanslanmalıdır. Teklif edilen lisansların süresi en az 5 yıl olmalıdır.*	
10.12.	The system to be proposed should be able to work with all network devices that are IEEE 802.1x compliant and independent of the brand.	*Teklif edilecek sistem, IEEE 802.1x uyumlu marka bağımsız tüm ağ cihazları ile çalışabilmelidir.*	
10.13.	The system to be proposed should be able to authorize MAC for devices that do not support IEEE 802.1x.	*Teklif edilecek sistem, IEEE 802.1x desteği olmayan cihazlar icin MAC yetkilendirmesi yapabilmelidir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
11. Firewall		***Güvenlik Duvarı***	**Brand/Model //** ***Marka/Model:***
11.1.	The proposed system must have at least the following features as the next	*Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari aşağıdaki özelliklerde olmaldır.*	

	generation firewall features. • Firewall • IPSec VPN Termination System • SSL VPN Termination System • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control • URL Category Filtering • Bandwidth management	• *Güvenlik Duvarı (Firewall)* • *IPSec VPN Sonlandırma Sistemi* • *SSL VPN Sonlandırma Sistemi* • *Saldırı Tespit ve Engelleme Sistemi (IPS)* • *Uygulama Tanıma ve Kontrolü (Application Control) Sistemi* • *Virüs/Zararlı İçerik Kontrolü* • *URL Kategori Filtreleme* • *Bant genişliği yönetimi*	
11.2.	These features should be provided with a single device as a hardware solution of the manufacturer. However, in case IPSec VPN and SSL VPN features cannot be supported when positioned Transparent; It can be provided with the virtual firewall feature on the same system or with a separate hardware product from the same manufacturer.	*Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlanmalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.*	
11.3.	The device can operate as a single physical firewall, and	*Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği*	

	in any case, it must be configured to run at least 10 virtual firewalls if the organization needs it.	*gibi, her halukarda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.*	
11.4.	The proposed Network Firewall must support Active-Active and Active-Passive operation for High-Availability. It should be able to share load while Active-Active. In case of failure of one of the devices, the other device should be able to continue operating by undertaking all functions.	*Teklif edilen Ağ Güvenlik Duvarı, High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.*	
11.5.	The system must have SPI (Stateful Packet Inspection) Firewall feature.	*Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.*	
11.6.	The system will detect and block spoofed packets.	*Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır.*	
11.7.	Each of the network interfaces in the system; It must be able to be defined as LAN, WAN, DMZ, or user-nameable segments. The system should support IEEE 802.1Q VLAN and defined VLANs should be used as an interface.	*Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN'lar arayüz (interface) olarak kullanılabilmelidir*	
11.8.	When offered with System Virtual Firewall feature; Physical and virtual interfaces on the system should be able to be shared between Virtual Firewalls. Virtual Firewalls should be managed independently from each other in terms of rules and routing.	*Sistem Sanal Güvenlik Duvarı özelliği ile teklif edildiği durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilmelidir.*	

11.9.	System; It must be able to work on Layer3 (routing mode) and Layer2 (transparent mode) layers. While the desired virtual firewall systems on the system can work in Layer3, the desired virtual firewalls must be able to work transparently on Layer2 at the same time.	*Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.*	
11.10.	It should provide the following features in Transparent mode: • SPI (stateful packet inspection), • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control on Gateway • URL Category Filtering	*Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır:* • *SPI (stateful packet inspection),* • *Saldırı Tespit ve Engelleme Sistemi (IPS)* • *Uygulama Tanıma ve Kontrolü (Application Control) Sistemi* • *Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü* • *URL Kategori Filtreleme*	
11.11.	In routing mode, it should provide the following features: • SPI (stateful packet inspection), • IPSec VPN Termination,	*Routing modda aşağıdaki özellikleri sağlamalıdır;* • *SPI (stateful packet inspection),* • *IPSec VPN Sonlandırma,* • *SSL VPN Sonlandırma,*	

	• SSL VPN Termination, • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control • URL Category Filtering • Bandwidth control • Static routing, • RIP must support OSPF and BGP routing protocols. If a license or extra software is required to provide these routing protocols, it must have been provided. • Server load balancing • WIFI Access Point controller • WAN optimization	• *Saldırı Tespit ve Engelleme Sistemi (IPS)* • *Uygulama Tanıma ve Kontrolü (Application Control) Sistemi* • *Virüs/Zararlı İçerik Kontrolü* • *URL Kategori Filtreleme* • *Bant genişliği kontrolü* • *Statik yönlendirme (static routing),* • *RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.* • *Sunucu yük dengeleme* • *WIFI Access Point kontrolcüsü* • *WAN optimizasyon*	
11.12.	The Network Security System should support multiple Wide Area Network (WAN) connections, and be able to use more than one Internet	*Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet*	

	connection as redundant.	*bağlantısını yedekli olarak kullanabilmelidir.*	
11.13.	Network Security System must support Policy Based Routing.	*Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.*	
11.14.	The system must have DHCP Server and DHCP Relay feature.	*Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.*	
11.15.	Firewall policies should be able to be written on the network interface and / or zone basis on the system.	*Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü ve/veya zone bazlı yazılabilmelidir.*	
11.16.	Firewall policies should be written on the basis of user and user groups. Must have AD integration for user information.	*Güvenlik duvarı politikaları, kullanıcı ve kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.*	
11.17.	The system should be able to do rule-based traffic shaping and traffic prioritization for Bandwidth Control. The system must support QoS and Differentiated Services. • Traffic formatting should also be defined in rules written on the basis of source, destination, and protocol (such as SMTP, FTP, DNS, H323). • The maximum and	*Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme, ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.* • *Kaynak, hedef, ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.* • *Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta,*	

	/ or guaranteed bandwidth value should be defined by priority value (such as low, medium, high). • Bandwidth control on per-IP basis should be possible when required. In this way, it should be ensured that the bandwidth defined for each resource allowed on the same rule is guaranteed. • Contrary to Article abone, it should be ensured that the bandwidth defined for each resource allowed within the same rule can be used in common. • It should be able to control bandwidth on the basis of application. • Bandwidth control should be possible in inbound and outbound direction	*yüksek gibi) ile tanımlanabilmelidir.* • *İstenildiğinde per-IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural üzerinden izin verilen her kaynak için tanımlanan bant genişliğinin garanti edilmesi sağlanmalıdır.* • *Üstteki maddenin aksine tüm aynı kural dahilinde izin verilen her kaynak için tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.* • *Uygulama bazında bant genişliği kontrolü yapabilmelidir.* • *Aynı trafik ile ilgili Inbound ve outbound doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant*	

	for the same traffic. Thus, while bandwidth can be specified in the outbound line for a permitted connection, a different bandwidth should be applied for the traffic corresponding to this connection.	*genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.*	
11.18.	Security System; It must be able to authenticate and authorize over the user database defined on it, RADIUS and LDAP.	*Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.*	
11.19.	The system must have application control feature. System; It should be able to recognize, control and block traffic of at least 3,000 (three thousand) applications, such as messaging (such as MSN, ICQ, Yahoo, AOL), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella, etc.) and Web Applications, regardless of the port used. . Applications recognized within the scope of application control should be updated with an update service over the internet.	*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.*	
11.20.	It should be possible to control whether the policy-	*Politika bazlı firewall'un oturumlarda start/stop*	

	based firewall logs start / stop in sessions .	*loglayıp / loglamaması denetlenebilmelidir.*	
11.21.	Firewall, NAT, and all layer7 security functions provided should be able to be enabled in granular form on a rule-based basis "only for traffic that meets the specified criteria."	*Firewall, NAT ve sunulan tüm layer7 güvenlik fonksiyonları granüler şekilde "sadece belirlenen kriterlere uyan trafik için" kural bazlı devreye alınabilmelidir.*	
11.22.	Daily operation operations should be able to be performed to a large extent (without the need to operate on the CLI) via WebGUI. On the other hand, the entire configuration should be able to be intervened in bulk via CLI.	*WebGUI üzerinden günlük operasyon işlemleri büyük oranda (CLI üzerinde işlem yapmaya gerek olmadan) gerçekleştirilebilmelidir. CLI üzerinden ise tüm konfigürasyona bulk şekilde müdahale edilebilmelidir.*	
11.23.	The application control policy should be set in each firewall rule written on the basis of source (IP and / or user), target, service.	*Kaynak (IP ve/veya kullanıcı), hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.*	
11.24.	The system should support IPSec VPN as VPN Gateway. DES must support MD5 and SHA-1 with 3DES, AES Encryption. There should be support for IKE and PKI. IPSEC VPN functions should be able to perform at hardware level performance on special ASIC-architecture hardware without straining the main resources of the system.	*Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır. IPSEC VPN işlevleri ASIC mimarili özel hardware üzerinde sistem ana kaynaklarını yormadan donanımsal seviyede performanslı gerçekleştirilebilmelidir.*	
11.25.	The IPS system should be able to detect and stop Traffic and Protocol anomalies , as well as recognize and stop	*IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları*	

	signature-based attacks. IPS signatures should be able to be updated automatically with the update service over the internet. The update process should also be able to be done manually.	*otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilmelidir.*	
11.26.	It should allow system administrators to create and block weakness signatures specific to the organization / need .	*Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkan sağlamalıdır.*	
11.27.	IPS policy should be set in every firewall rule written on the basis of source (IP and / or user), target, service.	*Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.*	
11.28.	The proposed Network security system should be able to detect and block Botnet activity.	*Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.*	
11.29.	By analyzing the behavior of user traffics, it should allow easy detection of user machines displaying abnormal behavior on the graphical interface. All behaviors between layer3-layer7, such as traffic blocked through the firewall, attempts to access inappropriate web categories, running risky applications, communication with botnet sites, should be determined by weighing determinable scoring. In this way, it is aimed to detect a zero-day activity	*Kullanıcı trafiklerinin davranış analizini yaparak, anormal davranış gösteren kullanıcı makinalarının grafiksel arayüzde kolayca tesbitine olanak sağlamalıdır. Firewall üzerinden bloklanan trafikler, uygunsuz web kategorilerine erişim denemeleri, riskli uygulamaların çalışıyor olması, botnet siteleri ile haberleşme gibi layer3-layer7 arası tüm davranışlar ağırlığı belirlenebilir puanlama ile belirlenebilmelidir. Bu sayede henüz imzası yayınlanmamış bir sıfır-gün aktivitesinin tesbit edilmesi amaçlanmaktadır*	

	whose signature has not yet been published.		
11.30.	The Network Security System must have SSL VPN Gateway feature in order to provide secure access of Mobile Users to Institution resources. SSL VPN client must support at least Windows, Mac OS, Linux operating systems and IOS, Android based mobile devices.	*Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.*	
11.31.	TCP and UDP-based traffic must be tunneled through SSL VPN Gateway.	*SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.*	
11.32.	SSL VPN feature will be offered with unlimited user license.	*SSL VPN özelliği sınırsız kullanıcı lisansı ile teklif edilecektir.*	
11.33.	Users accessing via SSL VPN should be able to authenticate and authorize over the user database defined on the System, RADIUS, LDAP, and define internal and external resources that can be accessed with this authorization.	*SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.*	
11.34.	For users or systems accessing with SSL VPN and IPSEC VPN; SPI (stateful packet inspection), Intrusion Detection and Prevention System (IPS), Application Recognition and Control (Application Control) System, Virus / Malicious Content Control and URL Category Filtering, QoS and Bandwidth management features must be applicable.	*SSL VPN ve IPSEC VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, QoS ve Bant Genişliği yönetimi özellikleri uygulanabilir olmalıdır.*	

11.35.	Malware detection and blocking feature must be available on the Network Firewall System. System; It should be able to prevent malicious software by scanning HTTP, SMTP, FTP, and POP3, IM (ICQ, MSN, Yahoo Messenger), MAPI, HTTPS, SMTPS, POP3S, IMAPS, FTPS, SMB traffic. The system scans within the aforementioned protocols; It should be able to detect and stop threats such as Worm, Trojan, Keylogger, Spy, Dialer. Virus Control should be able to be performed between all network segments on the Network Firewall System. The AntiVirus system should be able to automatically update virus signatures over the Internet.	*Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3, IM (ICQ, MSN, Yahoo Messenger) , MAPI, HTTPS, SMTPS, POP3S, IMAPS, FTPS, SMB trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir*	
11.36.	AV control policy should be set in every firewall rule written on the basis of source (IP and / or user), target, service.	*Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.*	
11.37.	There should be URL Filtering feature on the Network Security System. In this way, Category - based URL Filtering should be able to. Different categories of URL filtering should be able to be applied to different users and user groups.	*Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.*	
11.38.	Different URL filtering policies should be set for each firewall rule written on the basis of source (IP	*Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında*	

	and / or user), target, and service.	*farklı URL filtreleme politikaları set edilebilmelidir.*	
11.39.	At least 75 URL categories on the system and more than 250 million were categorized URL should contain.	*Sistem üzerinde en az 75 adet URL kategorisi ve 250 milyondan fazla kategorize edilmiş URL bulunmalıdır.*	
11.40.	There should be no user limit for the URL Filtering function of the system and should be offered with an unlimited user license.	*Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.*	
11.41.	Apart from URL filtering categories, the addresses requested as wildcard, regex, or full URL should be defined under different profiles (such as * .gov.tr *). Access to these defined addresses should be blocked or allowed.	*URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.*	
11.42.	URL filtering warning screens can be customized.	*URL filtreleme uyarı ekranları özelleştirilebilecektir.*	
11.43.	All systems offered must have IPv6 support and support dual-stack feature, which allows the use of IPv4 and IPv6 protocols at the same time. At least under IPv6; IPv6 addressing, IPv6 static routing, IPv6 DNS, IPv6 security rules, IPv6 recording and reporting, and Ping6 must be supported. IPS, Application Control, and Web Filtering should be able to be applied to IPv6 traffic.	*Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir. IPv6 trafiğine IPS, Uygulama Denetimi ve Web Filtreleme yapılabilmelidir.*	

11.44.	System configuration should be able to be done by at least the following methods: • With serial connection, through the console port, • With Http and Https connection, via web interface or via the manufacturer's own Linux or Windows based management application • With SSH connection, via the command line	*Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:* • *Seri bağlantı ile konsol port üzerinden,* • *Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden* • *SSH bağlantı ile komut satırı (command line) üzerinden*	
11.45.	Network Firewall The system must support SNMP and must support SNMPv3	*Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir*	
11.46.	Network Firewall System operating system and software updates must be made via the Web interface, TFTP or FTP.	*Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.*	
11.47.	Updates of systems running redundantly should be able to be made at least via web gui. Systems should be able to be automatically updated	*Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak*	

	sequentially without disrupting traffic.	*şekilde sırayla güncellenebilmelidir.*	
11.48.	There should be no user limit for the system about the Firewall, VPN, IPS functions and should be offered with an unlimited user license. Licenses to perform Software / operating system updates for 3 years and IPS, Application Recognition and Control, AntiVirus, URL Category Filtering services and updates for at least 3 years of the Network Security System must be provided with the system.	*Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.*	
11.49.	The recommended firewall system manufacturer must have one or more of its products, entered the "NSS Labs Network IPS" and "NSS Labs Next Generation Firewall" tests and should be in the recommended product category.	*Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, "NSS Labs Network IPS" ve "NSS Labs Next Generation Firewall" testlerine girmiş ve tavsiye edilen ürün kategorisinde olması gereklidir.*	
11.50.	The Firewall System must have a geographic database. It should be able to cut the traffic from the specified country or countries by writing a rule on a country basis.	*Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.*	
11.51.	The proposed security system will also have load balancing features. • It should be able to load balance all sessions based on HTTP, HTTPS, SSL	*Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.* • *Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP , Layer 3 için IP protokolü*	

	for Layer 7, TCP and UDP for Layer 4, and IP protocol for Layer 3.
	• IPS, AV policies should be available for servers with load balancing.
	• For HTTP and HTTPS connections, the source IP address should be able to go to physical servers.
	• Must have SSL Offloading feature for SSL connections.
	• Traffic should be able to be distributed to the real servers of the institution by the following methods:
	  • Source IP hash information
	  • Round robin
	  • By making a weight definition in the real server definitions against the possibility of
		bazında tüm oturumlar için yük dengelemesi yapabilmelidir.
		• *Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.*
		• *HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.*
		• *SSL bağlantıları için SSL Offloading özelliği olmalıdır.*
		• *Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:*
		  • *Kaynak Ip hash bilgisi*
		  • *Round robin*
		  • *Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak*
		  • *Aktif durumda olan gerçek sunuculardan*	

	the servers having different powers • The traffic is sent to the first of the active real servers and the load is sent to the next active server in case of inactivity. • Based on responses to ping packets • Depending on the session number information directed to the servers • During load sharing, it should be able to check server availability by tcp, http (eg checking http://190.1.128.1/ test_page.htm), and ping.	*ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi* • *Ping paketlerine verilen cevaplar esas alınması* • *Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak* *Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin http://190.1.128.1/test_page.htm adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.*	
11.52.	It should be able to perform vulnerability scanning tests on specified systems.	• *Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.*	
11.53.	The proposed system can work as a wifi controller, so it can be used for the	*Teklif edilen sistem wifi controller olarak çalışabilecek, bu sayede kullanılabilecek*	

	management of wireless access devices that can be used.	*kablosuz erişim cihazlarının yönetimi için kullanılabilecektir.*	
11.54.	Wan will have optimization features.	*Wan optimizasyon özelliklerine sahip olacaktır.*	
11.55.	It should be able to optimize the protocol for Common Internet File System (CIFS), FTP, HTTP, MAPI, and TCP sessions.	*Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.*	
11.56.	Must have web cache feature.	*Web cache özelliği olmalıdır.*	
11.57.	It must support Web cache communication Protocol (WCCP).	*Web cache communication Protocol (WCCP) desteği olmalıdır.*	
11.58.	Proposed security system should have at least 10/10/6 Gbps Firewall performance value for 1518/512/64 Byte IP packet size in the proposed configuration. These values should be stated in the documentation for the product offered and the manufacturer should have posted these values publicly on his website.	*Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, 1518/512/64 Byte IP paket büyüklüğü için en az 10/10/6 Gbps Firewall performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.*	
11.59.	The system must support at least 700 thousand sessions at the same time and must have a performance of at least 35 thousand new sessions per second. These values should be specified in the product documentation offered. These values should be stated in the documentation for the product offered and the	*Sistem aynı anda en az 700bin oturumu desteklemeli ve saniyede en az 35 Bin yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün belgelerinde belirtilmiş olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.*	

	manufacturer should have published these values publicly on his website.		
11.60.	Firewall System must have at least 6.5 Gbps IPSec VPN throughput for AES128 + SHA-1 . These values should be stated in the documentation for the product offered and the manufacturer should have published these values publicly on his website.	*Güvenlik Duvarı Sisteminin AES128 + SHA-1 için en az 6.5 Gbps IPSec VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.*	
11.61.	The system must support 200 Site-to-Site and at least 500 IPSec VPN tunnels for Client-to-Site. The device must be able to work compatible with VPN Gateway devices that comply with the standards that support the aforementioned VPN protocols.	*Sistem Site-to-Site 200 adet ve Client-to-Site için en az 500 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir*	
11.62.	The system must have a performance rating of 1.4 Gbps IPS throughput. This value should be stated in the documentation for the product offered, and the manufacturer should have posted these values publicly on his website.	*Sistem 1.4 Gbps IPS throughput performans değerine sahip olmalıdır. Bu değer teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.*	
11.63.	There should be at least 5 10/100/1000 Base-T and 2 Management Port ports on the system.	*Sistem üzerinde En az 5 adet 10/100/1000 Base-T, 2 adet Management Port bağlantı noktası olmalıdır.*	
11.64.	The system must be able to send records to the Syslog Servers, to the Registration / Reporting System that will	*Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama*	

	be offered with the System, and to keep records.	*Sistemine kayıt gönderebilmeli kayıt tutabilmelidir.*	
11.65.	Log and Hotspot software that fully complies with the Law No. 5651 should be offered with the system.	*Sistemle birlikte 5651 nolu kanunu tam karşılayan Log ve Hotspot yazılımı teklif edilmelidir.*	
11.66.	The proposed system must have a software and hardware warranty of at least 3 years. Licenses to perform Software / Firmware updates for 3 years must be given with the system.	*Teklif edilen sistemin en az 3 yıl yazılım ve donanım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
12. Personal Computer		***Bilgisayar***	**Brand/Model //** ***Marka/Model:***
12.1.	The computer to be offered must be a corporate product. The warranty period should be extended with additional packages.	*Teklif edilecek bilgisayar kurumsal ürün olmalıdır. Garanti süresi ek paketler ile uzatılabilmelidir.*	
12.2.	The frame size of the computer must be in MFF form.	*Bilgisayarın kasa tipi MFF formunda olmalıdır.*	
12.3.	The processor of the computer should have a minimum 2.2 GHz base CPU speed.	*Bilgisayarın işlemcisi en az 2.2 GHz temel hızında olmalıdır.*	

12.4.	The computer's RAM memory must be at least 4GB.	*Bilgisayarın RAM hafızası en az 4GB olmalıdır.*	
12.5.	The disk capacity of the computer must be at least 500GB.	*Bilgisayarın disk kapasitesi en az 500GB olmalıdır.*	
12.6.	The operating system of the computer must be Windows 10 Pro or equivalent.	*Bilgisayarın işletim sistemi Windows 10 Pro ya da eşdeğeri olmalıdır.*	
12.7.	There should be at least 4 USB 3.1 ports and at least 2 USB 2.0 ports on the computer. At least 2 of the USB ports should be located on the front of the case.	*Bilgisayarın üzerinde en az 4 adet USB 3.1 portu ve en az 2 adet USB 2.0 portu bulunmalıdır. USB portlarının en az 2 tanesi kasanın ön tarafında konumlandırılmalıdır.*	
12.8.	The computer must have at least 1 RJ-45 ethernet port.	*Bilgisayarın en az 1 adet RJ-45 ethernet portu bulunmalıdır.*	
12.9.	There should be at least 1 HDMI 1.4 and at least 1 DisplayPort 1.2 port on the computer for Monitor connection.	*Bilgisayarın üzerinde Monitör bağlantısı için en az 1 adet HDMI 1.4 ve en az 1 adet DisplayPort 1.2 portu bulunmalıdır.*	
12.10.	There should be headphone and microphone jacks on the computer.	*Bilgisayarın üzerinde kulaklık ve mikrofon girişleri bulunmalıdır.*	
12.11.	DVD-RW must be on the computer.	*Bilgisayar üzerinde DVD-RW bulunmalıdır.*	
12.12.	The computer must have at least 2 M.2 slots.	*Bilgisayarın en az 2 adet M.2 yuvası bulunmalıdır.*	
12.13.	At least 23.8 ”monitor of the same brand should be provided with the computer.	*Bilgisayar ile birlikte aynı marka en az 23.8” monitör verilmelidir.*	

12.14.	The monitor must support 1920 x 1080 60Hz resolution.	*Monitör 1920 x 1080 60Hz çözünürlüğü desteklemelidir.*	
12.15.	The brightness of the monitor should be at least 250cd / m2.	*Monitör ün parlaklığı en az 250cd/m2 olmalıdır.*	
12.16.	The response time of the monitor should be at most 6ms.	*Monitör ün tepkime süresi en çok 6ms olmalıdır.*	
12.17.	The monitor should have a depth of 16.7 Million colors.	*Monitör 16.7 Milyon renk derinliğine sahip olmalıdır.*	
12.18.	The monitor should be visible horizontally and vertically at an angle of at least 178 degrees.	*Monitör yatayda ve dikeyde en az 178 derecelik açıda görülebilmelidir.*	
12.19.	The monitor should be height adjustable.	*Monitörün yüksekliği ayarlanabilir olmalıdır.*	
12.20.	The monitor must have anti-glare properties.	*Monitör parlama önleyici özelliğe sahip olmalıdır.*	
12.21.	The same brand of wireless keyboard and wireless mouse should be given with the computer.	*Bilgisayar ile birlikte aynı marka kablosuz klavye ve kablosuz Mouse verilmelidir.*	
12.22.	The individual computer and monitor must have a warranty period of at least 3 years.	*Teklil edilen bilgisayar ve monitör en az 3 yıl garanti süresine sahip olmalıdır.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
13. Data Center Security Software		***Veri Merkezi Güvenlik Yazılımı***	**Brand/Model //** ***Marka/Model:***

13.1.	All components that make up the Data Center Security Software to be offered will be a single product from the same manufacturer. Even if it belongs to the same manufacturer, it will not be a solution created by combining different products.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımını oluşturan tüm bileşenler aynı üreticiye ait tek bir ürün olacaktır. Aynı üreticiye dahi ait olsa farklı ürünlerin bir araya getirilmesinden oluşturulan bir çözüm olmayacaktır.*	
13.2.	The Data Center Security Software to be offered will be capable of managing the security policies of server systems in physical, virtual, and cloud environments from a single point.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı fiziksel, sanal ve bulut ortamdaki sunucu sistemlerin güvenlik politikalarını tek bir noktadan yönetebilecek özellikte olacaktır.*	
13.3.	The Data Center Security Software to be offered should be offered to license 10 servers.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı 10 adet sunucuyu lisanslayacak şekilde teklif edilmelidir.*	
13.4.	The Data Center Security Software to be offered will consist of Central Management System and Operating system agent applications.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi ve İşletim sistemi ajan uygulamalarından oluşacaktır.*	
13.5.	The Data Center Security Software to be offered will be able to run on the following operating system platforms: • Windows Server 2016 (64-bit) • Windows Server 2012 or 2012 R2 (64-bit) — Full Server or Server Core • Windows Server 2008 R2 (64-bit) • Windows Server 2008 (32-bit and 64-bit)	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı aşağıdaki işletim sistemi platformlarında çalışabilecektir:* • *Windows Server 2016 (64-bit)* • *Windows Server 2012 or 2012 R2 (64-bit) — Full Server ya da Server Core* • *Windows Server 2008 R2 (64-bit)* • *Windows Server 2008 (32-bit ve 64-bit)*	

	• Windows Server 2003 SP2 or higher (32-bit and 64-bit) • Windows 10 or 10 TH2 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 7 (32-bit and 64-bit) • Windows XP (32-bit and 64-bit) • Hyper-V on Windows 2012 R2, 2012, 2008 R2, 8, and 8.1 • Red Hat Enterprise Linux 7 (32-bit and 64-bit) • Red Hat Enterprise Linux 6 (32-bit and 64-bit) • Red Hat Enterprise Linux 5 (32-bit and 64-bit) • CentOS 7 (32-bit and 64-bit) • CentOS 6 (32-bit and 64-bit) • CentOS 5 (32-bit and 64-bit) • Oracle Linux 7 (32-bit and 64-bit) • Oracle Linux 6 (32-bit and 64-bit) • Oracle Linux 5 (32-bit and 64-bit) • SUSE Enterprise Linux 12 (64-bit) • SUSE Enterprise Linux 11 SP1, SP2, and SP3 (32-bit and 64-bit) • CloudLinux 7 (32-bit and 64-bit) • CloudLinux 6 (32-bit and 64-bit) • Debian 7 (64-bit) • Debian 8 (64-bit) • Ubuntu 16.04 LTS (64-bit) • Ubuntu 14.04 LTS (64-bit)	• *Windows Server 2003 SP2 ya da daha yükseği (32-bit ve 64-bit)* • *Windows 10 or 10 TH2 (32-bit ve 64-bit)* • *Windows 8.1 (32-bit ve 64-bit)* • *Windows 8 (32-bit ve 64-bit)* • *Windows 7 (32-bit ve 64-bit)* • *Windows XP (32-bit ve 64-bit)* • *Hyper-V on Windows 2012 R2, 2012, 2008 R2, 8, ve 8.1* • *Red Hat Enterprise Linux 7 (32-bit ve 64-bit)* • *Red Hat Enterprise Linux 6 (32-bit ve 64-bit)* • *Red Hat Enterprise Linux 5 (32-bit ve 64-bit)* • *CentOS 7 (32-bit ve 64-bit)* • *CentOS 6 (32-bit ve 64-bit)* • *CentOS 5 (32-bit ve 64-bit)* • *Oracle Linux 7 (32-bit ve 64-bit)* • *Oracle Linux 6 (32-bit ve 64-bit)* • *Oracle Linux 5 (32-bit ve 64-bit)* • *SUSE Enterprise Linux 12 (64-bit)* • *SUSE Enterprise Linux 11 SP1, SP2, ve SP3 (32-bit and 64-bit)* • *CloudLinux 7 (32-bit ve 64-bit)* • *CloudLinux 6 (32-bit ve 64-bit)* • *Debian 7 (64-bit)* • *Debian 8 (64-bit)* • *Ubuntu 16.04 LTS (64-bit)* • *Ubuntu 14.04 LTS (64-bit)*	

	• Solaris 11, 11.2, or 11.3 (64-bit, SPARC, or x86) • Solaris 10 Update 11 (64-bit, SPARC, or x86)	• *Solaris 11, 11.2, or 11.3 (64-bit, SPARC, ya da x86)* • *Solaris 10 Update 11 (64-bit, SPARC, ya da x86)*	
13.6.	The Data Center Security Software to be offered should support working in a highly accessible architecture.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı yüksek erişilebilir mimaride çalışmayı desteklemelidir.*	
13.7.	The Data Center Security Software Central Management System to be proposed must support working on the following operating systems: • Windows Server 2016 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit) • Red Hat Enterprise Linux 7 (64-bit)	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi aşağıdaki işletim sistemleri üzerinde çalışmayı desteklemelidir:* • *Windows Server 2016 (64-Bit)* • *Windows Server 2012 (64-Bit)* • *Windows Server 2012 R2 (64-Bit)* • *Red Hat Enterprise Linux 7 (64-Bit)*	
13.8.	The Data Center Security Software to be proposed should support working with the following systems as the Central Management System database. • Oracle Database 12c, • Microsoft SQL Server 2016 • Microsoft SQL Server 2014,	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi veritabanı olarak aşağıdaki sistemler ile çalışmayı desteklemelidir.* *Oracle Database 12c, Microsoft SQL Server 2016 Microsoft SQL Server 2014, Microsoft SQL Server 2012, Postgre SQL 9.6 (Core Distribution & Amazon RDS) Microsoft SQL RDS ya da Oracle RDS*	

	• Microsoft SQL Server 2012, • Postgre SQL 9.6 (Core Distribution & Amazon RDS) • Microsoft SQL RDS or Oracle RDS		
13.9.	On the Data Center Security Software to be offered, there will be intrusion detection and prevention, firewall, malware prevention, website reliability, integrity monitoring, log inspection, and application control components, and all components related to these functions will be offered.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde saldırı tespit ve önleme, güvenlik duvarı, zararlı yazılım önleme, web sitesi güvenilirliği, bütünlük gözleme, kütük inceleme ve uygulama kontrolü bileşenleri bulunacak, bu işlevlerle ilgili tüm bileşenler teklif edilecektir.*	
13.10.	The attack detection and prevention component to be found on the Data Center Security Software to be proposed will be in an architecture that can scan incoming and outgoing traffic and work with deep packet inspection (DPI).	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak saldırı tespit ve önleme bileşeni gelen ve giden trafiği tarayabilecek ve derin paket inceleme (DPI) çalışabilecek mimaride olacaktır.*	
13.11.	Virtual Patch functionality on Windows systems will be supported by the intrusion detection and prevention module that will serve on the proposed Data Center Security Software . When necessary, modules provided at network level can be switched to "monitoring" mode.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde hizmet verecek olan saldırı tespit ve önleme modülü marifeti ile Windows sistemler üzerinde Sanal Yama işlevi desteklenecektir. Gerektiği durumlarda ağ seviyesinde sağlanan modüller "izleme" moduna alınabilecektir.*	

13.12.	The Data Center Security Software to be offered will include the virtual patch (host based IPS) feature. With the virtual patch feature, network vulnerabilities on the servers can be detected, and they can be turned off manually or automatically, optionally.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı, sanal yama (host based IPS) özelliğini barındıracaktır. Sanal yama özelliği ile sunucular üzerinde bulunan ağ zafiyetleri tespit edilebilecek, isteğe bağlı olarak manuel veya otomatik olarak kapatılabilecektir.*	
13.13.	The firewall component to be found on the Data Center Security Software to be proposed must be capable of preventing denial of service attacks (DoS) and discovery scans.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak olan güvenlik duvarı bileşeni hizmet dışı bırakma saldırılarını (DoS) ve keşif taramalarını engelleme yeteneğine sahip olmalıdır.*	
13.14.	Integrity monitoring component to be found on the proposed Data Center Security Software will be able to monitor and report changes in critical operating system files, directories, registry keys, and values in real-time and generate alarms.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak bütünlük gözleme bileşeni kritik işletim sistemi dosyaları, dizinleri, kayıt defteri (registry) anahtar ve değerlerindeki değişiklikleri gerçek zamanlı izleyerek rapor edebilecek, alarm üretebilecektir.*	
13.15.	The log analysis component to be found on the Data Center Security Software to be proposed will be able to monitor the log records and logs of the operating system and applications on the operating system it is running on, and report suspicious situations and generate alarms.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak kütük inceleme bileşeni çalıştığı işletim sistemi üzerindeki işletim sistemi ve uygulamalara ait günlük kayıtları ve kütükleri izleyerek şüpheli durumları rapor edebilecek, alarm üretebilecektir.*	
13.16.	The Data Center Security Software to be offered will be able to access the manufacturer's Global	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı üreticinin Global Tehdit İstihbarat hizmetine erişebilecek, bu*	

	Threat Intelligence service, and with this service, it will be able to make reputation inquiries for web pages, electronic mail resources, and files.	*hizmet sayesinde web sayfaları, elektronik posta kaynakları ve dosyalar için saygınlık sorguları yapabilecektir.*	
13.17.	The Data Center Security Software to be offered will support integration with the same manufacturer's Detailed Analysis System for Advanced Attacks. With this integration, they will be able to send suspicious files for analysis. It will also be able to block files and URLs found as a result of the analysis.	*Teklif edilecek Veri Merkezi Güvenlik Yazılımı, aynı üreticinin Gelişmiş Saldırılar İçin Detaylı Analiz Sistemi ile entegrasyonu destekleyecektir. Bu entegrasyon ile şüpheli gördüğü dosyaları analize gönderebilecektir. Ayrıca analiz sonucu bulunan dosya ve URL leri bloklayabilecektir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
14. User Security Solution		***Kullanıcı Güvenliği Çözümü***	**Brand/Model //** ***Marka/Model:***
14.1.	All components to be offered will belong to the same manufacturer.	*Teklif edilecek tüm bileşenler aynı üreticiye ait olacaktır.*	
14.2.	The "User Security" solution to be offered will be offered for at least 15 end users.	*Teklif edilecek "Kullanıcı Güvenliği" çözümü en az 15 son kullanıcı için teklif edilecektir.*	
14.3.	The Anti-malware Software to be offered must support the endpoint platforms listed below.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı aşağıda listelenen uç nokta platformlarını desteklemelidir.* • *Windows 7 SP1*	

	• Windows 7 SP1 • Windows 8.1 • Windows 10 • Windows Server 2008R2 (64bit) • Windows Server 2012 (64bit) • Windows Server 2012R2 (64bit) • Windows Server 2016 (64bit) • Windows Server 2019 (64bit)	• *Windows 8.1* • *Windows 10* • *Windows Server 2008R2 (64bit)* • *Windows Server 2012 (64bit)* • *Windows Server 2012R2 (64bit)* • *Windows Server 2016 (64bit)* • *Windows Server 2019 (64bit)*	
14.4.	The Anti-malware to be offered should support the database platforms listed below. • Microsoft SQL Server 2008 Express SP2 • Microsoft SQL Server 2008 • Microsoft SQL Server 2008R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 Express SP1 • Microsoft SQL Server 2016 • Microsoft SQL Server 2016 SP1 • Microsoft SQL Server 2016 SP2	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı aşağıda listelenen veritabanı platformlarını desteklemektedir.* • *Microsoft SQL Server 2008 Express SP2* • *Microsoft SQL Server 2008* • *Microsoft SQL Server 2008R2* • *Microsoft SQL Server 2012* • *Microsoft SQL Server 2014* • *Microsoft SQL Server 2016 Express SP1* • *Microsoft SQL Server 2016* • *Microsoft SQL Server 2016 SP1* • *Microsoft SQL Server 2016 SP2* • *Microsoft SQL Server 2017*	

	• Microsoft SQL Server 2017		
14.5.	The Anti-malware Management server to be offered must be accessed and managed through the Web interface.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim sunucusuna Web ara yüzünden erişilmeli ve yönetim sağlanabilmelidir.*	
14.6.	The communication between the Malware Prevention Software management server to be offered and the agent software to run on the end user systems must be encrypted in the AES-256 encryption standard.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim sunucusu ile son kullanıcı sistemler üzerinde çalışacak ajan yazılımı arasındaki iletişim AES-256 şifreleme standardında şifreli olarak gerçekleştirilebilmelidir.*	
14.7.	The anti-malware software to be offered must be able to fully protect the operating systems on which it works against viruses, trojans, worms, and spyware, and must be able to provide full protection against malicious codes spreading over the network.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde çalıştığı işletim sistemlerini virüs, truva atı, worm ve spyware lere karşı tam olarak koruyabilmeli ve network üzerinden yayılan zararlı kodlara karşıda tam koruma sağlayabilmelidir.*	
14.8.	The Malware Prevention Software to be offered will monitor the suspicious file encryption activities of such malicious software on client systems in order to detect ransomware type malware and will be able to stop these encryption activities by quarantining or terminating them.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ransomware türünde zararlı yazılımları tespit etmek üzere, bu tip zararlı yazılımların istemci sistemler üzerindeki şüpheli dosya şifreleme faaliyetlerini izleyecek ve bu şifreleme faaliyetlerini karantinaya alarak ya da sonlandırarak durdurabilecektir.*	
14.9.	The Malware Prevention Software to be offered will be able to work with predictive machine	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı öngörüsel makine öğrenme yöntemi ile çalışabilecek, virüs imzalarına*	

	learning method and detect malicious software without the need for virus signatures.	*ihtiyaç duymadan zararlı yazılımları tespit edebilecektir.*	
14.10.	The Anti-malware Software to be offered should be able to provide kernel-level protection against rootkits.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı rootkitlere karşı kernel seviyesinde koruma sağlayabilmelidir.*	
14.11.	The Malware Prevention Software to be offered should provide a website rating service that will provide desktop level protection against web threats. With this feature, users should warn and block access before accessing web pages with harmful content.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı web tehditlerine karşı desktop seviyesinde koruma sağlayacak olan web sitesi derecelendirme hizmet alabilmesini sağlamalıdır. Bu özellik ile kullanıcıların, zararlı içerikli olan web sayfalarına erişmeden önce uyarmalı ve erişim engellemesi sağlamalıdır.*	
14.12.	In addition to malicious content sites that are blocked by the proposed Anti-Malware website rating feature, system administrators should be able to create their own allowed and banned lists.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı web sitesi derecelendirme özelliğinin engellediği zararlı içerikli sitelere ek olarak, sistem yöneticileri, kendi izinli ve yasaklı listelerini oluşturabilmelidir.*	
14.13.	The Malware Prevention Software to be offered should contain signatures and algorithms that can detect malicious codes, especially with different compression methods.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı özellikle farklı sıkıştırma metotları ile kendini içine saklayan zararlı kodları tespit edebilecek imzaları ve algoritmaları içerisinde barındırmalıdır.*	
14.14.	The Anti-malware Software to be offered must include a stateful firewall.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı stateful özellikli bir güvenlik duvarı barındırmalıdır.*	

14.15.	The firewall on the Anti-malware to be offered should protect against DoS attacks and Syn Flood attacks.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan güvenlik duvarı, DoS ataklarına, Syn Flood ataklarına karşı koruma sağlamalıdır.*	
14.16.	All settings made on the proposed Anti-Malware Software should be backed up by the central management software and easily recycled from the previously purchased backup when necessary.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde yapılan tüm ayarlar merkezi yönetim yazılımı yolu ile yedeklenebilmeli ve gerektiğinde kolayca daha önce alınmış yedekten geri döndürülebilmelidir.*	
14.17.	With the Malware Prevention Software to be offered, in case of a virus epidemic, shares and port access on the network should be closed with rules to be sent manually. Write rights on the file and folder should be able to be turned off.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile herhangi bir virüs salgını durumunda ağ üzerindeki paylaşımlar ve port erişimleri el ile yollanacak kurallarla kapatılabilmelidir. Dosya ve klasör üzerindeki yazma hakları kapatılabilmelidir.*	
14.18.	With the Anti-malware Software to be offered, all virus, spyware and software updates should be done centrally and can be sent to clients remotely, automatically and manually.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile tüm virüs, spyware ve yazılım güncellemeleri merkezi olarak yapılmalı ve istemcilere uzaktan otomatik ve el ile yollanabilmelidir.*	
14.19.	The Malware Prevention Software to be offered should have the infrastructure to ensure that the manually downloaded update files are applied to the central server even if the central server does not have an internet connection.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı merkezi sunucunun internet bağlantısı olmasa dahi el ile indirilen güncelleme dosyalarının merkezi sunucuya uygulanmasını sağlayacak alt yapıya sahip olmalıdır.*	

14.20.	Anti-malware to be offered, mobile users should be able to keep their software under protection with their roaming profile when they are not connected to the center. At the same time, these users should be able to make updates via their internet connection without the need for central management software.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı mobil kullanıcılar merkez ile bağlantıları olmadığı zamanlarda gezici profili ile yazılımları koruma altında olmaya devam edebilmelilerdir. Aynı zamanda bu kullanıcılar merkezi yönetim yazılımına gerek kalmadan bulundukları internet bağlantısı yoluyla güncellemelerini yapabilmelilerdir.*	
14.21.	With the Anti-malware to be offered, POP3 e-mail connections should also be able to be checked for malware.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile POP3 e-posta bağlantıları da zararlı yazılımlara karşı denetlenebilmelidir.*	
14.22.	The Anti-malware Software to be offered should constantly monitor the activity on the computer whenever a file is opened or run, whenever any changes are made to the file (such as renaming, storing, moving, or copying to a directory or a directory) by looking at the virus signature definitions.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı bilgisayar üzerindeki aktiviteyi herhangi bir dosya açıldığında veya çalıştırıldığında, dosyada herhangi bir değişiklik yapıldığında (yeniden isimlendirme, saklama, taşıma veya bir dizine veya bir dizinden kopyalama gibi) virüs imza tanımlarına bakarak devamlı gözlemlemelidir.*	
14.23.	Anti-malware to be offered, the user will be able to scan for viruses on usb disk, hard disk, CDROM, and network drives.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcı usb disk, hard disk, CDROM ve ağ sürücüleri üzerinde virüs taraması yapabilecektir.*	
14.24.	Anti-malware to be offered will provide external device usage policies for users. There will be authorization rules for users to authorize	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcılar için harici aygıt kullanım politikaları sağlayacaktır. Kullanıcılar için harici aygıt kullanım yetkilendirilmesini*	

	the use of external devices.	*sağlayan yetki kuralları mevcut olacaktır.*	
14.25.	The Anti-malware Prevention Software to be offered will have heuristic scan feature. In this way, files that do not have a signature but are suspected of being viruses can be blocked.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı sezgisel tarama (heuristic scan) özelliğine sahip olacaktır. Bu sayede imzası bulunmayan ancak virüs olmasından şüphelenilen dosyalar bloklanabilecektir.*	
14.26.	The Anti-malware Software to be offered will also check for viruses in compressed (zip, etc.) files.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı sıkıştırılmış (zip vb.) dosyalarda da virüs denetimi yapacaktır.*	
14.27.	The Anti-malware Software to be offered should support the definition of exception rules so that the desired files and folders are not scanned during scans.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı taramalar sırasında istenilen dosya ve klasörlerin taranmaması için istisna kurallarının tanımlanmasını desteklemelidir.*	
14.28.	The Malware Prevention Software to be offered should be able to alert the system administrator via e-mail if the threshold value determined in any virus outbreak or malicious code attacks on the network is exceeded.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı herhangi bir virüs salgını ya da ağ üzerinde yaşanan zararlı kod saldırılarında belirlenen eşik değeri geçilmesi durumunda sistem yöneticisini e-posta yoluyla uyarabilmelidir.*	
14.29.	The Anti-malware to be offered should provide flexibility in processor (CPU) usage during security scans, and include maximum usage level settings.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı güvenlik taramaları sırasında işlemci (CPU) kullanımı konusunda esneklik sağlamalı, maksimum kullanım düzeyi ayarlarını içeresinde barındırmalıdır.*	
14.30.	Anti-Malware user components to be offered must be able to be installed via MSI packages. MSI packages should be able to be modified and recreated	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcı bileşenleri MSI paketleri yoluyla kurulabilmelidir. MSI paketleri değiştirilebilmeli ve*	

	with installation options.	*kurulum seçenekleri ile yeniden yaratılabilmelidir.*	
14.31.	The Malware Prevention Software to be offered should support the installations of operating systems from the image.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile imajdan işletim sistemleri kurulumlarını desteklenmelidir.*	
14.32.	The Anti-malware Software to be offered should support the reverting to previous versions of the virus update file and the malware scanning engine, both on the client and server side, in case of any problem. (Rollback)	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı herhangi bir sorun anında virüs güncelleme dosyasının ve zararlı tarama motorunun hem istemci hem de sunucu tarafında, bir önceki eski sürümlerine geri dönülmesini desteklemelidir. (Rollback)*	
14.33.	Virus, system update, event log, instant virus scanning, etc. on the Anti-malware Management software to be offered. Event records of information should be kept. The storage duration of the event logs on the management software should be determined by the system administrator.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim yazılımı üzerinde virüs, sistem güncelleme, olay günlüğü, anlık virüs tarama vb. bilgilere ait olay kayıtları tutulmalıdır. Yönetim yazılımı üzerinde olay kayıtlarının saklanma süresi, sistem yöneticisi tarafından belirlenebilmelidir.*	
14.34.	The Anti-malware Prevention Software to be offered will be automatically deleted from the system if inactive clients are detected within the specified day-out period.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı zaman aralığı verilerek belirlenen gün aşımında aktif olmayan istemciler tespit edildiği takdirde otomatik olarak sistemden silinmesi sağlanacaktır.*	
14.35.	The Anti-malware to be offered should be able to alert the system administrator via e-mail and SNMP as soon as they	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı, istemciler üzerinde zararlı bulunduğu anda e-posta ve SNMP yoluyla*	

	are found malicious on clients .	*sistem yöneticisini uyarabilmelidir.*	
14.36.	It should be possible to specify how long the logs will remain in the system on the Anti-malware Prevention Software to be offered, and optimize the log records by defining the automatic deletion process.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde üretilen logların sistemde ne kadar süre kalacağı belirtilebilmeli ve otomatik silme işlemi tanımlanarak log kayıtları üzerinde optimizasyon sağlanabilmelidir.*	
14.37.	With the Malware Prevention Software to be offered, the management features of the software to be installed on the clients can be customized by the system administrator through the central management software. The removal of the software from memory should be prevented, and its removal from the system by uninstall should be secured with password protection. The system administrator should be able to block access to the folders where the client software is installed, as well as to deny access within the registry.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile istemcilere yüklenecek yazılımların yönetim özellikleri merkezi yönetim yazılımı yoluyla sistem yöneticisi tarafından özelleştirilebilecektir. Yazılımın hafızadan çıkarılması engellenebilmeli, uninstall ile sistemden kaldırılması şifre korumalı olarak güvenlik altına alınabilmelidir. Sistem yöneticisi isterse istemci yazılımının kurulduğu klasörlere erişimleri engelleyebileceği gibi kayıt defteri içindeki erişimlerini de kesebilmelidir.*	
14.38.	Malware Prevention Software to be requested from the list of Spyware and Grayware should be considered as harmless and separated.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı Spyware ve Grayware listesinden istenilen yazılımlar zararsız olarak kabul edilip ayrıştırılabilmelidir.*	
14.39.	The Anti-malware Software to be offered must support receiving updates via proxy.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı proxy üzerinden güncellemeleri almayı desteklemelidir.*	

14.40.	Support the remote removal of agents located on endpoints with the Anti-malware Software to be offered.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile uç noktalar üzerinden bulunan ajanların uzaktan kaldırılmasını desteklemelidir.*	
14.41.	The infected files quarantined with the Anti-malware Prevention Software to be offered should be encrypted and stored.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile karantinaya alınan virüslü dosyalar şifrelenerek saklanmalıdır.*	
14.42.	More than one update source for the Anti-malware Software to be offered must be defined within the network. For this, an end-user computer with Malware Prevention Software agent installed on it should be used, and a separate computer should not be required for this feature.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı için birden fazla güncelleme kaynağı ağ içinde tanımlanabilmelidir. Bunun için üzerinde Zararlı Yazılım Önleme Yazılımı ajanı yüklü bir son kullanıcı bilgisayarı kullanılabilmeli, bu özellik için ayrı bir bilgisayar ihtiyacı olmamalıdır.*	
14.43.	Anti-malware to be offered should be integrated into the central product management software of the same manufacturer as required.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı gerektiğinde aynı üreticinin merkezi ürün yönetim yazılımına entegre olmalıdır.*	
14.44.	17.44. The Malware Prevention Software to be offered should be able to start time-dependent and instant scans on clients and monitor their results through the central management software.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı merkezi yönetim yazılımı yoluyla istemciler üzerinde zamana bağlı ve anlık taramalar başlatılıp sonuçları izlenebilmelidir.*	
14.45.	The Anti-malware Software to be offered should scan the entire network from a single point, detect clients with and without antivirus software installed, and	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı tek noktadan tüm ağı tarayarak antivirüs yazılımı kurulu olan ve olmayan istemcileri tespit etmeli, kurulu olmayan*	

	support the installation of an antivirus agent on clients that are not installed.	*istemcilere antivirüs ajanının kurulmasını desteklemelidir.*	
14.46.	The Malware Prevention Software to be offered should support the monitoring method such as changing the system registry keys, changing the host file, installing a new service, and changing existing services within the pre-determined policies by monitoring the changes made by the software that can be run on the client, and these monitoring settings should be edited separately for a specific group or a single client.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı istemci üzerinde çalıştırılabilecek olan yazılımların sistem üzerinde yapacakları değişiklikleri izleyerek daha önceden belirlenecek politikalar dahilinde sistem kayıt defteri anahtarlarının değiştirilmesi, host dosyasının değiştirilmesi, yeni bir servis yüklenmesi ve var olan servislerin değiştirilmesi gibi izleme metodunu desteklemeli ve bu izleme ayarları tüm sistem, belirli bir grup veya tek bir istemci için ayrı ayrı düzenlenebilmelidir.*	
14.47.	The Malware Prevention Software to be offered will be able to receive malicious URL, Domain, IP, and Hash information detected by the Detailed Analysis System for Advanced Attacks belonging to the same manufacturer as an update and share it with clients.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırılar için Detaylı Analiz Sistemi tarafından tespit edilen zararlı URL, Domain, IP ve Hash bilgisi güncelleme olarak alabilecek ve istemciler ile paylaşabilecektir.*	
14.48.	The Malware Prevention Software to be offered will be able to receive the SHA-1 control summary information of the malicious software detected by the Detailed Analysis System for Advanced Attacks belonging to the same manufacturer as an update over the Security	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırılar için Detaylı Analiz Sistemi tarafından tespit edilen zararlı yazılımların, şüpheli dosyaların SHA-1 kontrol özeti bilgilerini Güvenlik Yönetim Yazılımı üzerinden güncelleme olarak alabilecek ve bu zararlı yazılımları, şüpheli dosyaları*	

	Management Software, and will be able to clean these malicious software through the infected clients.	*bulaştığı istemciler üzerinden temizleyebilecektir.*	
14.49.	The Malware Prevention Software to be offered will be able to send suspicious files extracted from USB, e-mail and web pages to the Detailed Analysis System for Advanced Attacks of the same manufacturer, regardless of whether the client is in or out of the institution, for detailed analysis.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırılar için Detaylı Analiz Sistemi'ne istemcinin kurum içinde ya da kurum dışında olmasından bağımsız olarak USB, eposta ve web sayfalarından çekilmiş olan şüpheli dosyaları detaylı analiz amacı ile gönderebilecektir.*	
14.50.	Proposed Anti-Malware Software will be able to transmit event logs to a SIEM solution via syslog.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı olay kayıtlarını syslog aracılığıyla bir SIEM çözümüne iletebilecektir.*	
14.51.	Different administrator roles should be defined on the Anti-malware Prevention Software to be offered, and these users should be able to be pulled from Active Directory if desired.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde farklı yönetici rolleri tanımlanabilmeli ve bu kullanıcılar istenilirse Active Directory üzerinden çekilip kullanılabilmelidir.*	
14.52.	The Malware Prevention Software to be offered should be able to quickly generate detailed reports of the connected security software with ready report templates.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı hazır rapor şablonları ile hızlı bir şekilde bağlı bulunan güvenlik yazılımlarına ait detaylı raporlar üretebilmelidir.*	
14.53.	Anti-malware to be offered will provide external device usage policies for users. There will be authorization rules for users to authorize	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcılar için harici aygıt kullanım politikaları sağlayacaktır. Kullanıcılar için harici aygıt kullanım yetkilendirilmesini*	

	the use of external devices.	*sağlayan yetki kuralları mevcut olacaktır.*	
14.54.	Special reports will be provided in the Anti-malware Prevention Software to be offered.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımında özel raporlar alınması sağlanacaktır.*	
14.55.	The Malware Prevention Software to be offered will be able to generate reports in pdf, docx , xlsx formats.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı pdf,docx,xlsx formatlarında rapor üretebilecektir.*	
14.56.	Reports created with the Anti-malware Prevention Software to be offered should be able to be generated automatically depending on time.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile oluşturulan raporlar zamana bağlı olarak otomatik üretilebilmelidir.*	
14.57.	The Malware Prevention Software to be offered should be able to transmit the automatically generated reports to predetermined people by e-mail.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı otomatik oluşturulan raporları e-posta ile daha önceden belirlenmiş kişilere iletebilmelidir.*	
14.58.	The Anti-malware Software to be offered must have integrated data loss prevention (DLP) capability. • The data loss prevention system on the Anti-malware to be offered should have predefined data identifiers and templates and	*Teklif edilecek Zararlı Yazılım Önleme Yazılımı bütünleşmiş veri kaybı önleme özelliğine (DLP) sahip olmalıdır.* • *Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi ön tanımlı veri belirleyicileri ve şablonlara sahip olmalı ve kuruma özel belirleyici ve*	

	allow the identification of organization-specific identifiers and templates. • The data loss prevention system on the proposed Anti-Malware Software should be able to control access to certain applications and file types by default, and should be able to do this by recognizing the actual file type regardless of the file extension type. It should allow specific definitions for the institution to be made when necessary. • There must be a device control feature on the data loss prevention system on the Anti-malware Prevention Software to be	*şablonların tanımlanmasına olanak tanımalıdır.* • *Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi ön tanımlı olarak belirli uygulama ve dosya tiplerine erişimi denetleyebilmeli, bu işlemi dosya uzantısı tipinden bağımsız olarak gerçek dosya tipini tanıyarak yapabilmelidir. Gerektiğinde kuruma özel tanımlamaların yapılmasına olanak sağlamalıdır.* • *Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi üzerinde cihaz kontrol özelliği bulunmalıdır. Bu özellik ile istemciden farklı cihazlara doğru giden veriler uygulanan kurallara göre*	

	offered. With this feature, data traveling from the client to different devices should be blocked, allowed or recorded according to the rules applied. • The data loss prevention system on the Anti-malware Prevention Software to be offered must support the following data output channels. • Email Clients • FTP • HTTP and HTTPS • Instant communication applications (Instant Messaging) • SMB protocol • Webmail • Cloud storage services • CD / DVD • P2P applications • PGP encryption	*engellenebilmeli, izin verilebilmeli ya da kayıt altına alınabilmelidir.* • *Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi aşağıda belirtilen veri çıkış kanallarını desteklemelidir.* • *Email Clients* • *FTP* • *HTTP ve HTTPS* • *Anlık haberleşme uygulamaları (Instant Messaging)* • *SMB protokolü* • *Webmail* • *Bulut depolama servisleri* • *CD/DVD* • *P2P uygulamaları* • *PGP şifreleme* • *Printer* • *Harici veri depolama* • *ActiveSync* • *Windows Clipboard*	

	• Printer • External data storage • ActiveSync • Windows Clipboard		
14.59.	The Malware Prevention Software to be offered will have an intrusion detection and prevention feature (HIPS) and a virtual patching feature against zero-day attacks.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımında saldırı tespit ve engelleme özelliği (HIPS) ve sıfırıncı gün ataklarına karşı sanal yama yapma özelliği bulunacaktır.*	
14.60.	The Anti-malware to be offered will have an application control feature:	*Teklif edilecek Zararlı Yazılım Önleme Yazılımında uygulama kontrolü özelliği bulunacaktır:*	
14.61.	With the "lockdown" feature in the application control in the Malware Prevention Software to be offered, it will be able to learn the user's current inventory and only allow them to prevent new applications from running.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde "lockdown" özelliği ile kullanıcının mevcut envanterini öğrenip sadece onlara izin vererek, yeni uygulamaların çalışmasını engelleyebilecektir.*	
14.62.	Whitelist-blacklist rules can be created in the application control in the Anti-malware Prevention Software to be offered.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde whitelist-blacklist kurallar oluşturulabilecektir.*	
14.63.	In the application control in the Malware Prevention Software to be offered, blocking / allowing rules can be written according to the HASH information of the applications.	*Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde uygulamaların HASH bilgilerine göre bloklama/izin verme kurallar yazılabilecektir.*	

14.64.	The application control included in the Anti-malware Prevention Software to be offered can only work in logging mode	*Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolü sadece loglama modunda çalışabilecektir.*	
Item to be supplied description		***Tedarik edilecek ürün tanımı***	**Offered technical specifications by the Bidder shall be inserted in English** ***Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir***
15. Uninterruptable Power Supply		***Kesintisiz Güç Kaynağı***	**Brand/Model //** ***Marka/Model:***
15.1.	Bidding manufacturers must certify that they have the international ISO 9001-14001 and CE standard.	*Teklif veren üretici kuruluşlar Uluslararası ISO 9001-14001 ve CE standardına sahip olduklarını belgelemelidirler.*	
15.2.	In order not to affect computers and sensitive electronic systems, it must comply with the EN 62040-2 (EMC) standard, which minimizes electromagnetic effects, and the EN 62040-1 standard, which includes safety items.	*Bilgisayar ve hassas elektronik sistemlerin etkilenmemesi bakımından, elektromanyetik etkileri minumuma indiren EN 62040–2 (EMC) standardına ve güvenlik maddelerini içeren EN 62040–1 standardına uygun olmalıdır*	
15.3.	The offered product should be available in tower type and rack type when desired.	*Teklif edilen ürün istenildiğinde tower tip, istenildiğinde ise rack tipi kullanılabilmelidir.*	
15.4.	The company must provide the user manual and the service manual for maintenance and repair, written in Turkish language, free of charge, at the time of delivery of the	*Firma KGK' ların teslimi anında, herbir KGK için ayrı ayrı olmak üzere, kullanıcı el kitabını ve bakım onarım için servis el kitabını, Türkçe dilinde matbaa harfleriyle yazılmış halde ücretsiz olarak vermelidir.*	

	UPSs, separately for each UPS.		
15.5.	The UPSs will be an original model of the manufacturer's mass production. There will be no broken, cracked, scratched, paint defect, or deformed parts and will not be used.	*KGK 'lar imalatçının orijinal seri imalatı bir model olacaktırKırık, çatlak, çizik, boya hatası ve deformasyona uğramış hiçbir parçası bulunmayacak, kullanılmış olmayacaktır.*	
15.6.	State-of-the-art materials and elements should be used in the manufacture of UPSs.	*KGK' ların imalatında son teknoloji ürünü malzeme ve elemanlar kullanılmalıdır.*	
15.7.	All materials to be used in the assembly of UPSs must comply with TSE or international standards.	*KGK 'ların montajında kullanılacak tüm malzemeler TSE veya uluslararası standartlara uygun olmalıdır.*	
15.8.	Must have SNMP module.	*SNMP modülü olmalıdır.*	
15.9.	It should be able to be monitored with the Graphic Screen Remote Monitoring Panel when desired.	*İstenildiğinde Grafik ekranlı Uzaktan İzleme Paneli ile de izlenebilmelidir.*	
15.10.	Optionally, the MODBUS system must be compatible.	*Opsiyonel olarak MODBUS sistemi uyumlu olmalıdır.*	
15.11.	The Uninterruptible Power Supplies offered must be designed online and with DSP Control.	*Teklif edilen Kesintisiz Güç Kaynakları online olarak tasarlanmış ve DSP Kontollü olmalıdır.*	
15.12.	The UPS must have a Boost charging system.	*KGK Boost şarj sistemine sahip olmalıdır.*	
15.13.	UPSs should give the output power in kVA clearly and continuously in the Technical specification.	*KGK'lar, Teknik şartname de kVA cinsinden verilen çıkış gücünü net ve sürekli olarak vermelidir.*	

15.14.	UPS's; It should consist of rectifier, inverter, battery charger, static and manual by-pass switch main units.	*KGK 'lar; Redresör, İnvertör, Akü şarjörü, Statik ve Manuel By-pass Şalteri ana ünitelerinden oluşmalıdır.*	
15.15.	The rectifier must have been manufactured using IPM technology. While providing the necessary DC voltage for the inverter, it should also be able to charge the batteries.	*Redresör IPM teknolojisi kullanılarak üretilmiş olmalıdır. İnvertör için gerekli DC gerilimi sağlarken aynı zamanda aküleri de şarj edebilmelidir.*	
15.16.	The inverter must be manufactured using IGBT technology and must continuously feed the load by converting the DC energy received from the rectifier or battery pack into AC energy. The inverter should operate synchronously with the grid within the limits specified in the synchronization parameters. In case of inverter failure or overload, it should transfer the load to the grid without interruption in the load supply.	*İnvertör, IGBT teknolojisi kullanılarak imal edilmiş olmalıdır ve redresörden yada akü gurubundan aldığı DC enerjiyi AC enerjiye çevirerek, sürekli olarak yükü beslemelidir. İnvertör, senkronizasyon parametrelerinde belirtilen sınırlar içinde şebekeye senkron çalışmalıdır. İnvertör arızasında veya aşırı yük durumunda, yük beslemesinde kesinti olmaksızın yükü şebekeye aktarmalıdır.*	
15.17.	The battery pack must provide the necessary DC energy to the inverter in case the mains fails or the grid goes out of the specified tolerance. In case the network returns or returns within limits, the rectifier should automatically supply DC energy and the battery charger should start	*Şebekenin kesildiği veya şebekenin belirtilen tolerans dışına çıkması durumunda akü grubu invertere gerekli DC enerjiyi sağlamalıdır. Şebekenin geri gelmesi veya limitler içine dönmesi durumunda, redresör otomatik olarak DC enerjiyi sağlamalı, akü şarjörü akü grubunu şarj etmeye başlamalıdır.*	

	charging the battery group.		
15.18.	In order to save energy in the proposed uninterruptible power supplies, economical operating mode (Ecomode) should be optional.	*Teklif edilen Kesintisiz güç kaynaklarında enerji tasarrufu amacıyla opsiyonel olarak ekonomik çalışma modu (Ecomode) olmalıdır.*	
15.19.	In case of failure, the UPS should be able to disable itself depending on the location and nature of the failure. The faults should be visible on the panel on the UPS with the illuminated LEDs or on the LCD panel.	*Arıza durumunda, arızanın yerine ve mahiyetine gore KGK kendisini devre dışı bırakabilmelidir. Arızalar KGK üzerindeki panelden ışıklı LED 'lerle veya LCD panel üzerinden görülebilmelidir.*	
15.20.	128 historical events and 5000 alarms must be able to be kept in the memory.	*Geçmişe yönelik 128 adet olay ve 5000 alarmı hafızada tutulabilmelidir.*	
15.21.	There should also be a manual by-pass unit in order to facilitate maintenance operations.	*Bakım işlemlerinde kolaylık sağlaması amacıyla ayrıca manuel by-pass ünitesi de bulunmalıdır.*	
15.22.	In order to facilitate maintenance / repair and minimize maintenance time, UPS's microprocessor circuits and circuit boards should be in easily accessible locations and in a replaceable manner in case of malfunction.	*Bakım/onarımın kolaylaştırılması ve bakım süresinin asgari seviyeye indirilmesi amacıyla KGK'ların mikroişlemci devreleri ile devre kartları kolay ulaşılabilir yerlerde ve arıza durumunda değiştirilebilir şekilde olmalıdır.*	
15.23.	UPS must be working in parallel at least up to 4 units.	*KGK' en az 4 adete kadar parelel çalişiyor olmak zorundadir.*	
15.24.	The technical service has to present the training	*Teknik servisin eğitim sertifikalarını teklif ekinde sunmak zorundadır.*	

	certificates in the offer attachment.		
15.25.	Input characteristics • Input Voltage and Tolerance : 220VAC (1Phase N) ± 20% • Input Frequency and Tolerance : 40-65hz • Bypass voltage and Tolerance : the first phase 220 ± 10% • System Input Power Factor : 0.99 • Input Current THD : <5%	*Giriş karakteristikleri* • *Giriş Gerilim ve Toleransı :220VAC (1FAZ, N) ± %20* • *Giriş Frekansı ve Toleransı :40-65Hz* • *By-Pass Gerilimi ve Toleransı :220 1 faz ± %10* • *Sistem Giriş Güç Faktörü :0,99* • *Giriş Akım THD :<%5*	
15.26.	Output Characteristics • Output Power : 15 kVA • Power Kw : 10.5 kW • Output Waveform : sinusoidal • Output Voltage : 220 VAC • Output Voltage Tolerance : +/- 1% • Output Power Factor : 0.7 • Output Frequency : 50 Hz • Output Frequency Tolerance : +/-% 0.2 • Efficiency at 100% load :> 92% • Crest Factor : 3: 1 • Overload : 10 minutes at 100-125% load. • Output Voltage at Linear Load : <3% • Acoustic Noise : <50 dBA	*Çıkış Karakteristikleri* • *Çıkış Gücü :15 kVA* • *Güç Kw :10.5 kW* • *Çıkış Dalga Şekli : Sinusoidal* • *Çıkış Gerilimi : 220 VAC* • *Çıkış Gerilim Toleransı : +/- %1* • *Çıkış Güç Faktörü : 0,7* • *Çıkış Frekansı : 50 Hz* • *Çıkış Frekans Toleransı : +/- %0.2* • *Verim %100 yükte : >%92* • *Crest Faktörü : 3:1* • *Aşırı Yük : %100-125 yükte 10 dk.* • *Çıkış Gerilimi Lineer Yükte : < %3* • *Akustik Gürültü : < 50 dba*	

15.27.	It must be in a structure that can keep the battery group in float charge while feeding the inverter at full load by converting the one-phase alternating voltage received from the network to the regulated correct voltage.	*Şebekeden aldığı bir fazlı alternatif gerilimi regüle edilmiş doğru gerilime çevirerek invertörü tam yükte beslerken akü grubunu tampon şarjda tutabilecek yapıda olmalıdır.*	
15.28.	The rectifier must have soft start feature. The current drawn during soft start should not be more than the rated current of the device. Even if the input voltage is cut for a very short time (the situation where the rectifier DC bus does not reach zero completely), it should draw current in accordance with the soft start feature.	*Redresör soft start özelliğine sahip olmalıdır. Soft start esnasında çekilen akım cihazın anma akımından fazla olmamalıdır. Giriş geriliminin çok kısa süreli kesilmesinde dahi (doğrultucu DC barasının tamamen sıfıra erişmediği durum) soft start özelliğine uygun akım çekmelidir.*	
15.29.	In case of mains power cut, input voltage and frequency out of specified tolerance values, and in cases such as phase cut, the rectifier will be automatically deactivated and the inverter will be fed through the battery . In case the appropriate voltage and frequency to be provided from the network or generator is restored, the rectifier will automatically re-engage and feed the inverter.	*Şebeke enerjisinin kesilmesinde, giriş gerilim ve frekansının belirtilen tolerans değerleri dışına çıkmasında ve faz kesilmesi gibi durumlarda redresör otomatik olarak devreden çıkacak, invertör akü üzerinden beslenecektir. Şebeke veya jeneratörden sağlanacak uygun gerilim ve frekansın yeniden sağlanması durumunda redresör otomatik olarak tekrar devreye girerek invertörü besleyecektir.*	
15.30.	In order to prevent the battery cells from being damaged by excessive charging current, there will	*Akü hücrelerinin aşırı şarj akımı ile hasarlanmasının önlenmesi amacıyla, şarj*	

	be a current limiting circuit on the charge card.	*kartında akım sınırlama devresi bulunacaktır.*	
15.31.	Designed using IPM technology, the inverter must transfer the DC voltage from the rectifier or battery pack to a regulated and noise-free AC voltage and transfer it to the static transfer circuit.	*IPM teknolojisi kullanılarak tasarlanan invertör, redresör veya akü grubundan gelen DC gerilimi regüleli ve her türlü gürültüden arındırılmış bir AC gerilime çevirerek statik transfer devresine aktarmalıdır.*	
15.32.	The inverter should be manufactured as microprocessor controlled so that it will be continuously on.	*İnvertör sürekli olarak devrede kalacak şekilde mikro işlemci kontrollu olarak imal edilmiş olmalıdır.*	
15.33.	Output voltage should not exceed +/- 1% and frequency +/- 0.2 % (battery operation) tolerance limits.	*Çıkış gerilimi +/- %1 ve frekansı +/- %0.2 (Aküden çalışma) tolerans sınırlarını aşmamalıdır.*	
15.34.	The dynamic tolerance of the output voltage should not exceed +/- 5%. (At 100% load impulse) This tolerance should be set to ± 2% within 20 ms at the most.	*Çıkış geriliminin dinamik toleransı +/- %5 'i aşmamalıdır. (% 100 yük darbesinde) Bu tolerans en çok 20 msn'de ± % 2 sınırlarına çekilmelidir.*	
15.35.	Total harmonic amount of output voltage at full load should not exceed 3% in linear loads and 5% in computer loads (CF: 3:1).	*Tam yükte çıkış gerilimi toplam harmonik miktarı, lineer yüklerde % 3'ü, bilgisayar yüklerinde (CF: 3:1) %5 'ü geçmemelidir.*	
15.36.	The inverter output must be protected against short circuits.	*İnvertör çıkışı kısa devrelere karşı korunmuş olmalıdır.*	
15.37.	The inverter must have an overheat protection circuit.	*İnvertörde aşırı ısı koruma devresi bulunmalıdır.*	
15.38.	It must be an electronically controlled semiconductor switch consisting of semi-	*Yarı iletkenlerden meydana gelen elektronik kontrollü yarı iletken bir şalter olmalı ve KGK*	

	conductors and feed the load from the inverter in the normal operation of the UPS. In case of overload, short circuit, or a failure in the inverter, the load should be transferred to the network or auxiliary source without power cut. If the inverter also fails, it must transfer the load back to the inverter. If it is out of the specified tolerance value, it should not transfer to the network.	*' nın normal çalışması durumunda yükü invertörden beslemelidir. Aşırı yükte, kısa devre durumunda veya invertörde bir arıza meydana geldiğinde yükü enerji kesintisi olmaksızın şebekeye yada yardımcı kaynağa aktarmalıdır. Invertör de arıza geçmiş ise yükü tekrar invertöre aktarmalıdır. Belirlenen tolerans değeri dışında ise şebekeye transfer işlemini gerçekleştirmemelidir.*	
15.39.	As long as the grid is within the given tolerance limits, it should be able to perform automatic synchronization and phase locking with the inverter output. Otherwise, the inverter should be locked to its internal oscillator.	*Şebeke verilen tolerans sınırları içinde olduğu sürece invertör çıkışı ile aralarında otomatik senkranizasyon ve faz kilitlenmesi yapabilmelidir. Aksi durumda invertör kendi dahili osilatörüne kilitlenmelidir.*	
15.40.	From the LEDs on the front panel of the UPS or the LCD screen, it should be possible to learn whether the mains and the inverter output are synchronous , synchronous out-of-limit status and overload status.	*UPS ön panelindeki ledler veya LCD ekrandan, şebeke ile invertör çıkışının senkron olup olmadığını, senkron limit dışı durumunu ve aşırı yük durumunu öğrenilebilmelidir.*	
15.41.	Static transfer circuit should be able to automatically select the network or inverter under specified conditions. In synchronous operation, the transfer between the inverter and the grid should be possible without interruption.	*Statik transfer devresi belirtilen şartlarda şebeke veya invertör seçimini otomatik olarak yapabilmelidir. Senkron çalışmada, invertör ile şebeke arasındaki transfer kesintisiz yapılabilmelidir.*	

15.42.	When the UPS is requested to be disabled for maintenance, repair, or other reasons, it should transfer the load to the network or auxiliary source without interruption.	*Bakım, onarım veya başka sebeplerle KGK ' nın devre dışı bırakılması istenildiğinde yükü şebekeye yada yardımcı kaynağa kesintisiz aktarmalıdır.*	
15.43.	When this switch is ON, there should be no voltage at any point in the UPS cabinet other than the input terminals.	*Bu şalter ON durumunda iken KGK kabini içerisinde giriş terminallerinin dışında hiçbir noktada gerilim bulunmamalılıdr.*	
15.44.	When 220/380 V, 50 Hz mains power is cut or when the specified tolerance band is exceeded, the UPS should continue to supply the load from the dual polarity battery group. It should feed the system to be fed for 15 minutes at full load. No interruption should be felt in the output from the battery group to supply.	*220/380 V, 50 Hz şebeke enerjisi kesildiğinde yada belirtilen tolerans bandının dışına çıkıldığında KGK çift polariteli akü grubundan yükü beslemeye devam etmelidir. Beslenecek sistemi tam yükte 15 dk süreyle beslemelidir. Akü grubundan beslemeye geçişte, çıkışta herhangi bir kesinti hissedilmemelidir.*	
15.45.	Batteries; completely closed, maintenance-free, dry type, stationary (suitable for being under continuous charging) rechargeable, must have a life expectancy of at least 5 years.	*Aküler; tamamen kapalı, bakım gerektirmeyen (maintenance- free), kuru Tip, stasyoner (sürekli şarj altında kalmaya elverişli) şarj edilebilen, en az 5 yıl ömür beklentili olmalıdır.*	
15.46.	Information such as battery capacity used, battery charge voltage, and current should be monitored on the LCD panel on the device and from the software.	*Kullanılan akü kapasitesi , akü şarj voltajı ve akımı gibi bilgilerin cihazın üzerindeki LCD panelden ve yazılımdan izlenebilmelidir.*	
15.47.	Batteries necessary for the maintenance of the UPS System ' from separating	*Sistemin bakımı için gerektiğinde aküleri KGK 'dan ayıran anahtarlama sistemi*	

	switching system will be found. In this state, the UPS should continue to perform its functions without a battery.	*bulunacaktır. Bu durumda iken KGK aküsüz olarak fonksiyonlarını yerine getirmeye devam etmelidir.*	
15.48.	The calculation of the battery group should be made using the maximum power per cell method.	*Akü grubunun hesabı hücre başına düşen maksimum güç yöntemiyle yapılmalıdır.*	
15.49.	Battery connection parts will be insulated and not touch the body. Connections between blocks should be made of flexible material.	*Akü bağlantı parçaları izoleli ve gövdeye temas etmeyecek şekilde olacaktır. Bloklar arası bağlantılar esnek malzemeden yapılmalıdır.*	
15.50.	Rectifier, Bypass inputs, and Inverter output must be protected with a breaker or fuse in the system.	*Sistemde Doğrultucu, Bypass girişleri ve Evirici çıkışı şalter veya sigorta ile korunmalıdır.*	
15.51.	The inverter must be electronically protected against overload and short circuits.	*Aşırı yük ve kısa devreye karşı evirici elektronik olarak korunmalıdır.*	
15.52.	The system must have battery overcharge and discharge protection.	*Sistem, akü aşırı şarj ve deşarj korumasına sahip olmalıdır.*	
15.53.	The system must have over-heat protection.	*Sistem aşırı ısı korumasına sahip olmalıdır.*	
15.54.	The user should be able to access information about the operation of the system through the control panel of the UPS or the LCD screen. In addition, there should be a sound warning that can be silenced in case of failure or power failure.	*KGK' nın kontrol paneli veya LCD ekran üzerinden, kullanıcı sistemin çalışması ile ilgili bilgilere ulaşabilmelidir. Ayrıca arıza veya elektrik kesintisi durumunda susturulabilir ses ikazı olmalıdır.*	

15.55.	A connection with a computer must be possible with a standard RS 232 output. All information about the UPS should be displayed on the screen.	*Standart RS 232 çıkışı ile bilgisayar'la bağlantı kurulabilmelidir. KGK ile ilgili tüm bilgiler ekrandan izlenebilmelidir.*	
15.56.	As standard, the UPS should automatically shut down Novell, Windows, NT type operating systems when the electricity is cut off. The software to be provided for these operating systems must be graphic-based and given free of charge.	*Standart olarak UPS elektrikler kesildiğinde Novell, Wındows, NT, tipi işletim sistemlerini otomatik kapatabilmelidir. Bu işletim sistemleri için verilecek yazılım grafik tabanlı olmalı ve ücretsiz olarak verilmelidir*	
15.57.	The UPS must be compatible to be used with SNMP and communication must be made with SNMP when required.	*KGK SNMP ile kullanılmaya uyumlu olmalı ve istenildiğinde haberleşme SNMP ile yapılabilmelidir.*	
15.58.	The UPS system must have a firmware structure so that the system must be fully software controlled. Future developments should be able to be transferred to the system with the software development function and the system should be updated.	*KGK sistemi firmware yapısına sahip olmalı böylece sistem tamamı ile yazılım kontrollü olmalıdır. İleride olabilecek gelişmeler yazılım geliştirme fonksiyonu ile ile sisteme aktarılabilmeli ve sistem update edilebilmelidir.*	
15.59.	It should have automatic and manual battery test feature.	*Otomatik ve manuel akü test özelliği olmalıdır.*	
15.60.	The Uninterruptible Power Supply must be able to operate continuously between 0 °C and 40 °C, The working altitude must be up to 1000 m and at higher levels the system must operate with	*Kesintisiz GüçKaynağı 0□C ile 40□C arasında sürekli çalışabilmeli, Çalışma yüksekliği 1000 m'ye kadar olmalı ve daha yukarı seviyelerde sistem, fazla hava*	

	excessive air circulation.	*sirkülasyonu sağlamakla çalışmalıdır.*	
15.61.	The amount of heat the system emits into the environment should be specified.	*Sistemin ortama yaymakta olduğu ısı miktarı belirtilmelidir.*	
15.62.	The Uninterruptible Power Supply should have a front panel in liquid crystal display (LCD) structure.	*Kesintisiz Güç Kaynağında likit kristal display (LCD) yapısında bir ön panel bulunmalıdır.*	
15.63.	The user should be able to get information about the progress of the system at a glance from this panel. Control keys and other controller keys required for the system should also be located here.	*Kullanıcı bu panodan sistemin gidişatı hakkında bir bakışta bilgi sahibi olabilmelidir. Sistem için gerekli olan kontrol tuşları ile diğer kontrol edici anahtarlar da burada yer almalıdır.*	
15.64.	The following status and alarm messages must be visible on the front panel: • Load is on Uninterruptible Power Supply • Freight By-Pass also • Manual By-Pass •Emergency shutdown • The battery voltage is low • Fault codes • Audible alarm on • Mains cut • Overload • Excessive heat • Battery low • High Battery	*Ön panelde aşağıdaki durum ve alarm mesajları mutlaka görülebilmelidir:* • *Yük Kesintisiz Güç Kaynağında* • *Yük By-Pass da* • *Manuel By-Pass* • *Acil kapatma* • *Akü gerilimi düşük* • *Arıza kodları* • *Sesli alarm açık* • *Şebeke kesik* • *Aşırı yük* • *Aşırı ısı* • *Akü düşük* • *Akü yüksek* • *Çıkış düşük* • *Çıkış yüksek*	

	• Output low • Output high		
15.65.	In addition, the values below should be monitored on the LCD panel from the measurement menu: • Load value in% • Output voltage and frequency • Input voltage, current, and frequency • By-pass voltage and frequency • Input current • Battery voltage, battery discharge current • Battery capacity and remaining battery time • Temperature	*Ayrıca aşağıda bulunan değerler ölçüm menüsünden LCD panelde izlenebilmelidir.* • *% olarak yük değeri* • *Çıkış voltajı ve frekansı* • *Giriş voltajı, akımı ve frekansı* • *By-pass voltajı ve frekansı* • *Giriş akımı* • *Akü voltajı , şarj deşarj akımı* • *Akü kapasitesi ve kalan akü süresi* • *Sıcaklık*	

Product catalogue/brochure of the proposed brand/model showing detailed technical specifications of the goods should be submitted.

Other Related services and requirements *(based on the information provided in Section 5b)*	**Compliance with requirements**		**Details or comments on the related requirements**
	Yes, we comply	**No, we cannot comply** *(indicate discrepancies)*	
Delivery, installation and commissioning of each item within 90 calendar days following the signature of the contract			
Warranty (min. 3 years) for each item			
Local Service Support			
Training following installation			