

**ÜSKÜDAR ÜNİVERSİTESİ**

**DİŞ HEKİMLİĞİ PROJESİ**

**TEKNİK ŞARTNAMESİ**

**İÇİNDEKİLER**

1. **SUNUCU TEKNİK ŞARTNAMESİ**
   1. HİPER BÜTÜNLEŞİK SİSTEM TEKNİK GEREKSİNİMLERİ
   2. DİSK TABANLI YEDEKLEME SİSTEMİ TEKNİK GEREKSİNİMLERİ
   3. BACKUP SERVER TEKNİK GEREKSİNİMLERİ
   4. SUNUCU LİSANS TEKNİK GEREKSİNİMLERİ
   5. TOR SWİTCH TEKNİK GEREKSİNİMLERİ
2. **GÜVENLİK TEKNİK ŞARTNAMESİ**
   1. AĞ GÜVENLİK CİHAZI ( 2 Adet )
   2. AĞ GÜVENLİK CİHAZI MERKEZİ YÖNETİM , LOGLAMA VE RAPORLAMA MODÜLÜ
   3. HOTSPOT UYGULAMASI
   4. LOG YÖNETİM CİHAZI
   5. VERİ TABANI GÜVENLİĞİ ÇÖZÜMÜ
   6. UÇ NOKTA GÜVENLİĞİ ÇÖZÜMÜ
3. **NETWORK TEKNİK ŞARTNAMESİ**
   1. NETWORK AĞ ERİŞİM KONTROL SİSTEMİ
   2. 48 PORT POE KENAR ANAHTARLAR (37 ADET)
   3. OMURGA ANAHTARLAR (2 ADET)
   4. KABLOSUZ AĞ KONTROL CİHAZI (2 ADET)
   5. İÇ ORTAM KABLOSUZ YAYIN CİHAZI (120 ADET)
   6. NETWORK YÖNETİM YAZILIMI
   7. KABLOSUZ AĞ KONTROL CİHAZI (2 ADET)
   8. MASA IP TELEFON TİP- 1 (90 ADET)
   9. MASA TLEFONU TİP -2 (1 ADET)
   10. KABLOSUZ AĞ MASA TELEFONU TİP -3 (10 ADET)
   11. ÇAĞRI KONTROL SİSTEMİ
   12. SES GEÇİT ROUTER (1 ADET)
   13. GARANTİ ve DİĞER HUSUSLAR
4. **MASAÜSTÜ BİLGİSAYAR**
   1. MASAÜSTÜ BİLGİSAYAR - AIO TEKNİK GEREKSİNİMLERİ (120 Adet)
   2. MASAÜSTÜ MİNİ BİLGİSAYAR - (17 Adet)
   3. GARANTİ ve DİĞER HUSUSLAR
5. **MICROSOFT LİSANSLARI TEKNİK ŞARTNAMESİ**
6. **DİĞER KONULAR**
7. **FİNANSAL BİLGİLER**

# **Giriş ve Amaç**

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

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

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

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

# **Projenin Açıklaması ve Ön Kabuller**

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

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

# **Genel Koşullar**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tüm çalışmalarda aşağıdaki durumlarda toplantı yapılması gerekecektir.

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

# **İhtiyaç**

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

1. **SUNUCU TEKNİK ŞARTNAMESİ**
   1. **HİPER BÜTÜNLEŞİK SİSTEM TEKNİK GEREKSİNİMLERİ**
      1. Her bir işlemci 64-bit komut setini desteklemelidir.
      2. Sunucular Vmware tarafından VSAN yazılımının koşması için test edilmiş, onaylanmış sunucu yapılandırmasında olmalıdır. (VSAN Certified nodes)
      3. Sistem miktarı 4 Adet (4 Node) olmalıdır.
      4. Sunucu üzerinde en az 1 adet, en az 2.1 GHz çalışma hızında fiziksel işlemci olmalıdır.
      5. İşlemci en az 20 çekirdekli olmalıdır.
      6. Her bir işlemci üzerinde en az 27.5 MB L3 önbellek bulunmalıdır.
      7. Her bir işlemci en az 2 adet UPI (Ultra Path Interconnect) bağlantı sayısınına sahip olmalıdır.
      8. Sunucu üzerinde kullanılan her bir bellek DDR4 olacaktır.
      9. Sunucu üzerinde en az 3200 MT/s, en az toplam 256 GB kapasitesinde olan bellek bulunacaktır. Bellekler 64GB kit halinde teklife eklenecektir
      10. Sunucu üzerinde en az 24 adet bellek yuvası bulunacaktır.
      11. Bellek modülleri ECC (Error Check Correction) özelliğinde olacaktır.
      12. Sunucu ile beraber en az 2 adet, her biri en az 3.84TB kapasiteli, 2.5 inç boyutunda, SSD teknolojisinde disk ve en az 1 adet 400GB kapasiteli 2.5 inç boyutunda SSD teknolojisinde disk teklife dahil edilmelidir. Diskler çalışma esnasında sökülüp takılabilmelidir.
      13. Teklif edilecek sunucu üzerinde M.2 Boss contoller kart eklenecektir. En az 2 adet 240 GB 2 M.2 Sticks dahil olmalıdır.
      14. Teklif edilecek sunucu üzerinde RAID denetleyecisi bulunmalıdır. RAID kartı donanımsal olarak RAID 0/1/5/10/50 yapabilme yeteneğine sahip olmalıdır.
      15. Sunucu üzerinde en az 24 adet 2.5 inch disk yuvası bulunacaktır.
      16. Her bir sunucu üzerinde en az 2 adet 2 portlu 10/25GbE ethernet bağlantı noktası bulunacaktır.
      17. Her bir sunucu üzerinde en az 1 adet HBA330 Controller, 12Gbps Mini card bulunacaktır.
      18. Sunucu için gerekli PDU ve kabloları ile birlikte daha önce kullanılmamış olarak teslim edilecektir.
      19. Her bir sunucu üzerinde çalışma esnasında sökülüp takılabilen; en az 2 adet, herbiri 1100W gücünde yedekli güç kaynağı bulunmalıdır. Sunucu üzerine gerektiğinde en az 2 adet, herbiri 2400W gücünde yedekli güç kaynağı takılabilmelidir.
      20. Her bir sunucu için, çalışma esnasında sökülüp takılabilen en az 6 adet yedekli ve teklif edilen sistemin tüm fan yuvaları dolu olacak şekilde fanlar takılı bulunmalıdır.
      21. Sunucuda Trusted Platform Module 2.0 (TPM 2.0) desteği bulunmalıdır.
      22. Teklif edilecek sunucu üzerinde 1 adet VGA portu, 2 adeti arka tarafta ve 2 adeti ön tarafta olmak üzere toplam 4 adet USB portu bulunmalıdır.
      23. Teklif edilecek sunucu üzerinde en az 4 adet x8 PCIe slotu bulunmalıdır.
      24. Sunucular üzerine, Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi işletim sistemleri kurulabilecektir.
      25. Teklif edilecek sunucu üzerinde embedded olarak en az 16 MB belleğe sahip ve en az 1920\*1200 çözünürlüğü destekleyen grafik kartı bulunmalıdır.
      26. Teklif edilen sunucu üzerinde sistem kurulumu için gerekli dosyalar embedded olmalıdır ve herhangi bir disk, sürücü ye ihtiyaç olmadan embeded sistem üzerinden sistem kurulabilmelidir.
      27. Sunucu üzerinde sistem ismi, seri numarası, uzaktan yönetim IP numarası, güç tüketimi ve arızaların kolay tespit edilebilmesini sağlayan arıza bilgilerini gösteren LCD ekran ya da uyarı ışıkları bulunmalıdır.
      28. Sunucu üzerinde HTTPS ve SSLv2 sertifika ile erişim sağlayacak kendine ait 1 Gb hızında fiziksel bağlantı noktasına sahip uzaktan yönetim modülü bulunmalıdır.
      29. 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.
      30. 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.
      31. Sunucular sanal medya özelliğini desteklemelidir, uzaktaki bir bilgisayara bağlı USB bellek, CD, DVD, vb. medyaları kullanabilmelidir.
      32. 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.
      33. 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.
      34. Teklif edilecek sunucu en az 2U boyutunda olmalı ve sunucunun çalışma esnasında kabinden öne çekilerek müdahale edilmesini sağlayacak üzerine baskı olduğunda eğilmesini engelleyecek aksesuarlara sahip metal alaşımlı kayan ray sistemi bulunmalıdır ve kablo yönetim kolu bulunmalıdır.
      35. Sunucu ile 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.
      36. 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.
      37. Sunucular en az 3 yıl boyunca 7x24 4Hr MC üretici garantisine sahip olacaktır.
   2. **DİSK TABANLI YEDEKLEME SİSTEMİ TEKNİK GEREKSİNİMLERİ**
      1. Teklif edilen disk tabanlı yedekleme sistemi yedeklenecek veriyi tampon bir disk alanına yazmaksızın doğrudan tekilleştirmelidir.
      2. Teklif edilen disk tabanlı yedekleme sistemi Gartner tarafından yayınlanan en yakın tarihli "Magic Quadrant for Deduplication Backup Target Appliances" raporunda liderler konumunda olmalıdır.
      3. Teklif edilen disk tabanlı yedekleme sistemi bir RAID grubunda aynı anda iki diskin arızalanmasına karşı koruma sağlamalıdır.
      4. Teklif edilen disk tabanlı yedekleme sistemi, yedeklenen verinin saklandığı alanı oluşturan disklerde arıza olması durumunda, arızalı diskin yerine otomatik olarak geçecek yedek (hot-spare) disk ya da diskler sağlamalıdır.
      5. Teklif edilen disk tabanlı yedekleme sistemi NAS (CIFS ve NFS) ve VTL protokollerinin aynı anda kullanımı için gereken tüm lisanslar sağlanacaktır.
      6. Teklif edilen disk tabanlı yedekleme sistemi, bir üst maddelerdeki protokoller haricinde üreticiye ait, daha hızlı yedekleme yapabilmek üzere geliştirilmiş bir protokole sahip olmalıdır. Bu protokol üreticinin desteklediği yedekleme yazılımları ile beraber kullanılabilmelidir. Özelleştirilmiş bu protokol için ek lisans gerekiyorsa teklife eklenecektir.
      7. Teklif edilen disk tabanlı yedekleme sistemi üzerinde aynı anda kullanılabilecek en az 50 adet yedekleme hedefi/cihazı (CIFS, NFS, VTL ve üretici özel protokol) yaratılabilecektir.
      8. Teklif edilen disk tabanlı yedekleme çözümü geriye dönük yedeklenmiş ve saklanmakta olan tüm verilerin düzenli olarak blok blok kontrolünü, kullanılabilecek yedekleme protokolüyle ilişkili cihaz tiplerinin (CIFS, NFS, VTL ve üretici özel protokol) hepsi üzerinde gerçekleştirmeli ve bozuk blokları otomatik olarak tespit ederek, dışarıdan müdahale olmaksızın otomatik olarak düzeltebilmelidir. Çözümün bu özelliği ne şekilde sağladığını açıklayan teknik belgeler teklif dosyasıyla birlikte sunulacaktır. Bu gereksinimi karşılayamayan çözümler, verinin güvenliğini sağlayabilmek için eşlenik bir sistem teklif etmeli ve verinin ikinci bir kopyasını tutarak veri güvenliğini sağlamalıdır.
      9. Teklif edilen disk tabanlı yedekleme sistemi üzerinde yaratılacak tüm cihazların (CIFS, NFS, VTL ve üretici özel protokol) hem kendi içinde hem de birbiri arasında global tekilleştirme desteği olacaktır. Bu teknolojiyi desteklemeyen çözümler düşük tekilleştirme sebebiyle oluşan kayıp duruma karşı %25 ek kapasite ile önerilecektir.
      10. Teklif edilen disk tabanlı yedekleme sistemi üzerinde tüm veri bütünlüğü denetimi ve düzeltme özellikleri aktif durumdayken, eş zamanlı gerçekleşecek yedekleme ve replikasyon işlemleri için 24 TB/saat'lik performans desteklenecektir.
      11. Teklif edilen disk tabanlı yedekleme sistemi 34 TB net kapasite ile sunulmalıdır. Sistem disk çekmecesi ekleme yoluyla en az 178 TB net kapasiteyi desteklemelidir.
      12. Teklif edilen disk tabanlı yedekleme sistemi üzerinde en az 4 adet 10 Gbit/sn hızında bakır temelli ağ bağlantı arabirimi bulunacaktır.
      13. Teklif edilen disk tabanlı yedekleme sistemi üzerinde en az 4 adet 10 Gbit/sn hızında optik temelli ağ bağlantı arabirimi bulunacaktır.
      14. Teklif edilen disk tabanlı yedekleme sistemi tek noktadan birden fazla noktaya ve birden fazla noktadan tek noktaya replikasyonu desteklemelidir. Bu özellikleri kullanmak için gereken tüm lisanslar sağlanacaktır.
      15. Teklif edilen disk tabanlı yedekleme sistemini merkezi olarak izlemek, yönetmek ve raporlamak için harici olarak kullanılacak bir yazılımı aracı sağlanacaktır. Bu araç aynı üreticiye ait olmak kaydıyla aynı anda birden fazla disk tabanlı yedekleme sistemi için kullanılabilecektir.
      16. Teklif edilen disk tabanlı yedekleme sistemi en az 3 yıl boyunca 7x24 4Hr MC üretici garantisine sahip olacaktır.
   3. **BACKUP SERVER TEKNİK GEREKSİNİMLERİ (1 ADET)**
      1. Her bir işlemci 64-bit komut setini desteklemelidir.
      2. Sunucu üzerinde en az 2 adet, en az 2.2 GHz çalışma hızında fiziksel işlemci olmalıdır.
      3. Her bir işlemci en az 10 çekirdekli olmalıdır. Sunucuda toplam olarak en az 24 çekirdek olmalıdır.
      4. Her bir işlemci üzerinde en az 13.5 MB L3 önbellek bulunmalıdır.
      5. Her bir işlemci en az 2 adet UPI (Ultra Path Interconnect) bağlantı sayısınına sahip olmalıdır.
      6. Sunucu üzerinde kullanılan her bir bellek PC4, DDR4 olacaktır.
      7. Sunucu üzerinde her biri 2933 MT/s, en az 16 GB kapasitesinde olan, toplamda en az 32 GB bellek bulunacaktır.
      8. Sunucu üzerinde en az 24 adet bellek yuvası bulunacaktır.
      9. Bellek modülleri ECC (Error Check Correction) özelliğinde olacaktır.
      10. Sunucu ile beraber en az 2 adet, her biri en az 480 GB kapasiteli, 2.5 inç boyutunda, SSD teknolojisinde disk teklife dahil edilmelidir. Diskler çalışma esnasında sökülüp takılabilmelidir.
      11. Teklif edilecek sunucu üzerinde elektrik kesilmesine karşı pil korumalı korumalı üzerinde en az 2 GB uçucu olmayan bellek bulunan RAID denetleyecisi bulunmalıdır. RAID kartı donanımsal olarak RAID 0/1/5/6/10/50/60 yapabilme yeteneğine sahip olmalıdır.
      12. Sunucu üzerinde en az 8 adet 2.5 inch disk yuvası bulunacaktır.
      13. Her bir sunucu üzerinde en az 2 adet 2 portlu 10Gb/25GbE SFP+ fiber ethernet portu bulunmalıdır.
      14. Sunucu için gerekli PDU ve kabloları ile birlikte daha önce kullanılmamış olarak teslim edilecektir.
      15. Her bir sunucu üzerinde çalışma esnasında sökülüp takılabilen; en az 2 adet, herbiri 750W gücünde yedekli güç kaynağı bulunmalıdır. Sunucu üzerine gerektiğinde en az 2 adet, herbiri 1100W gücünde yedekli güç kaynağı takılabilmelidir.
      16. Her bir sunucu için, çalışma esnasında sökülüp takılabilen en az 6 adet yedekli ve teklif edilen sistemin tüm fan yuvaları dolu olacak şekilde fanlar takılı bulunmalıdır.
      17. Sunucuda Trusted Platform Module 2.0 (TPM 2.0) desteği bulunmalıdır.
      18. Teklif edilecek sunucu üzerinde 1 adet VGA portu, 2 adeti arka tarafta ve 2 adeti ön tarafta olmak üzere toplam 4 adet USB portu bulunmalıdır.
      19. Teklif edilecek sunucu üzerinde en az 3 adet PCIe slotu bulunmalıdır.
      20. Sunucular üzerine, Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi işletim sistemleri kurulabilecektir.
      21. Teklif edilecek sunucu üzerinde embedded olarak en az 16mb belleğe sahip ve en az 1920\*1200 çözünürlüğü destekleyen grafik kartı bulunmalıdır.
      22. Teklif edilecek sunucu üzerine gerektiğinde aynı anda en az 3 adet Single width GPU kart takılabilmelidir.
      23. Teklif edilen sunucu üzerinde sistem kurulumu için gerekli dosyalar embedded olmalıdır ve herhangi bir disk, sürücü ye ihtiyaç olmadan embeded sistem üzerinden sistem kurulabilmelidir.
      24. Sunucu üzerinde sistem ismi, seri numarası, uzaktan yönetim IP numarası, güç tüketimi ve arızaların kolay tespit edilebilmesini sağlayan arıza bilgilerini gösteren LCD ekran ya da uyarı ışıkları bulunmalıdır.
      25. Sunucu üzerinde HTTPS ve SSLv2 sertifika ile erişim sağlayacak kendine ait 1 Gb hızında fiziksel bağlantı noktasına sahip uzaktan yönetim modülü bulunmalıdır.
      26. 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.
      27. 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.
      28. Sunucular sanal medya özelliğini desteklemelidir, uzaktaki bir bilgisayara bağlı USB bellek, CD, DVD, vb. medyaları kullanabilmelidir.
      29. 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.
      30. 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.
      31. Teklif edilecek sunucu en az 1U boyutunda olmalı ve sunucunun çalışma esnasında kabinden öne çekilerek müdahale edilmesini sağlayacak üzerine baskı olduğunda eğilmesini engelleyecek aksesuarlara sahip metal alaşımlı kayan ray sistemi bulunmalıdır ve kablo yönetim kolu bulunmalıdır.
      32. Sunucu ile 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.
      33. 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.
      34. Sunucular en az 3 yıl boyunca ertesi iş günü üretici garantisine sahip olacaktır. Garantinin üretici firma tarafından verildiğine dair yazı teklif dosyasında bulunmalıdır
   4. **LİSANS TEKNİK GEREKSİNİMLERİ**

# **Sanal Veri Depolama Yazılımı**

* + 1. Sanal veri depolama yazılımı, herhangi bir ek bileşen kullanmadan sanallaştırma katmanının yetenekleri ile dağıtık veri depolama sistemi kurabilme özelliğine sahip olmalıdır.
    2. Sanal veri depolama yazılımı 4 işlemciyi destekleyecek şekilde teklif edilecektir.
    3. Sanal veri depolama yazılımı, tüm kurulum yönetimini sunucu sanallaştırma yönetim yazılımı üzerinden yapabilmelidir.
    4. Sanal veri depolama yazılımı, sunucu sanallaştırma platformunda kullanılan dağıtık ağ anahtarı özelliğine ait lisansları içerecektir.
    5. Sanal veri depolama yazılımı, 1Gbit ve 10Gbit network bağlantılarını destekleyebilmeli, gerektiğinde yüksek performans beklentisi olmayan iş yükleri için 1Gbit üzerinde de çalışabilmelidir.
    6. Sanal veri depolama yazılımı, sanallaştırma yazılımının vMotion, HA, DRS, FT gibi özelliklerini performans kaybı olmadan desteklemelidir.
    7. Sanal veri depolama yazılımı, sanallaştırma yazılımı çekirdeği içinde çalışmalı ve sunucu üzerindeki disklere doğrudan erişebilmelidir.
    8. Sanal veri depolama yazılımı, SAS, SATA, NL-SAS, SSD ve NVMe diskleri desteklemelidir.
    9. Sanal veri depolama yazılımı, fiziksel sunucuların lokal disklerini istenirse hibrit (SSD ve Manyetik diskler birlikte), istenirse de tamamını SSD diskler kullanarak olmak üzere kullanabilmelidir.
    10. Sanal veri depolama yazılımı, IPv4 ve IPv6 desteğine sahip olmalıdır.
    11. Sanal veri depolama yazılımı, tüm sağlık, hata ve performans bilgisini sunucu sanallaştırma yönetim yazılımı üzerinden gösterebilme özelliğine sahip olmalıdır.
    12. Sanal veri depolama yazılımı, çalıştığı donanımlar ile uyumluluğunu kontrol edebilmeli, gerektiğinde uyumsuz donanım, sürücü ya da firmware bilgilerini raporlayabilmelidir.
    13. Sanal veri depolama yazılımı, 2 sunuculu ortamları destekleyebilmeli, 2 sunuculu ortamlarda sunucuların birbirlerine doğrudan kablo ile bağlanmasını destekleyebilmelidir.
    14. Sanal veri depolama yazılımı, 64 sunucuya kadar olan sunucu kümelerini destekleyebilmeli, yapıya benzer özellikli sunucular eklendikçe lineer performans kazanımı sağlanabilmelidir.
    15. Sanal veri depolama yazılımı, sanal depolama ortamına yeni sunucu ya da yeni disklerin sistemi kapatmadan eklenmesine imkan tanımalı, mevcut ortamın iş yükünü otomatik olarak yeni eklenen boş sunucu ya da disklere dağıtabilmelidir.
    16. Sanal veri depolama yazılımı, gerektiğinde sistem çalışırken ortamdan sunucu ya da disk çıkarılmasına imkan tanımalıdır, bu işlemler sırasında herhangi bir kesinti ya da veri kaybı yaşanmamalıdır.
    17. Sanal veri depolama yazılımı, poliçe tabanlı yönetimi desteklemeli, sanal makinaların ihtiyaç duydukları yedeklilik ve performans metrikleri poliçelerle le belirlenip sanal makinalara atanabilmelidir. Bu poliçeler istenirse sistem çalışırken düzenlenebilmeli ve çalışan bir sanal makinanın poliçesi kesintiye yola açmadan değiştirilebilmelidir.
    18. Sanal veri depolama yazılımı, gerektiğinde API ve Powershell üzerinden komutlar ile yönetime ve otomasyona imkan tanımalıdır.
    19. Sanal veri depolama yazılımı, sanal makine ve sanal disk seviyesinde RAID yapılmasına imkan tanımalıdır.
    20. Sanal veri depolama yazılımı, yüksek performanslı SSD. NVMe gibi diskleri okuma yazma ön belleği olarak kullanabilmeli ve bu ön bellek alanlarında istenen sanal makineler için önceliklendirme yapabilmelidir.
    21. Sanal veri depolama yazılımı, sunucular üzerine dağıtık RAID1 mimarisini desteklemelidir. İstenirse aynı verinin 1, 2 veya 3 kopyası saklanabilmelidir.
    22. Sanal veri depolama yazılımı, yazılım seviyesinde sanal makine bazlı snapshot ve klon operasyonlarını desteklemeli ve alınan snapshotların performansa etkisi minimumda olmalıdır.
    23. Sanal veri depolama yazılımı, RAID operasyonlarını yaparken sunucuların fiziksel olarak bulundukları rack kabinetleri hesaba katabilmeli, gerektiğinde herhangi bir kabindeki sunucuların tamamının kapanması durumunda dahi sitem veri kaybı olmaksızın çalışmaya devam edebilmelidir.
    24. Sanal veri depolama yazılımı, sunucu sanallaştırma katmanında yapılan replikasyon özelliğini desteklemeli, replikasyon aralığı 5 dakikaya kadar düşürülebilmelidir.
    25. Sanal veri depolama yazılımı, diskler üzerindeki bölümlerin fiziksel olarak bozulmalarına karşı yazlım tabanlı veri doğrulama/sağlama desteklemeli, bozulan bloklardaki veriyi kesintiye sebep olmadan onarabilmelidir. (Software Checksum)
    26. Sanal veri depolama yazılımı, sanallaştırma ortamı dışında kalan fiziksel sunucuların da sanal depolama alanında faydalanabilmeleri için iSCSI protokolü üzerinden erişime izin vermelidir.
    27. Sanal veri depolama yazılımı, gerektiğinde tek bir sanal makinenin ya da sanal diskin kullanabileceği en fazla disk performansını IOPS cinsinden belirleyebilmeli ve kısıtlayabilmelidir.
    28. Sanal veri depolama yazılımı all flash disk konfigürasyonlarında, tekilleştirme ve sıkıştırma işlevlerini desteklemelidir.
    29. Sanal veri depolama yazılımı, RAID5 ve RAID6 yedeklilik seviyelerini desteklemeli gerektiğinde farklı RAID seviyeleri arasında canlı geçişe imkan tanımalıdır.
    30. Teklif edilen çözüme ait lisanslar ile birlikte en az 1 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 1 yıl boyunca 7 gün 24 saat üretici destek hizmeti olmalıdır

# **Sanallaştırma Yazılımı**

* + 1. Teklif edilen sanallaştırma yazılımı aynı fiziksel sunucu üzerinde oluşturulacak sanal makinaların mevcut sistem kaynaklarının üzerinde kaynak atanmasına (over-commitment) izin vermelidir.
    2. Teklif edilen sanallaştırma yazılımı 4 işlemciyi destekleyecek şekilde teklif edilecektir.
    3. Teklif edilen sanallaştırma yazılımı SMP (Symetric Multi Processing) desteği olmalıdır. Teklif edilen sistemde her bir sanal makinaya istenildiğinde 128 adet sanal CPU atanabilmelidir.
    4. Teklif edilen sanallaştırma yazılımı ile her bir sanal makinaya 1TB sanal bellek atanabilmelidir.
    5. 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)
    6. Teklif edilen sanallaştırma yazılımı misafir işletim sistemi olarak Windows Xp, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Centos, Redhat, Ubuntu, Solaris, MacOSX, FreeBSD desteklemelidir.
    7. Teklif edilen sanallaştırma yazılımı, sanal makinalara verilen disklerin ve sanal makinaların bulunduğu dosya sisteminin sistem çalışırken büyütülmesine izin vermelidir.
    8. Teklif edilen sanallaştırma yazılımı sanal makinalara 62TB boyutunda sanal diskler atanmasına olanak sağlamalıdır.
    9. Teklif edilen sanallaştırma yazılımı 64TB boyutundaki depolama alanlarını yönetebilmelidir
    10. Teklif edilen sanallaştırma yazılımı ile FC, iSCSI ve NFS gibi veri depolama teknolojilerini ve bu teknolojilerle çalışan veri depolama ünitelerini desteklemelidir.
    11. 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.
    12. Teklif edilen sanallaştırma yazılımı ile sistem performansı CPU, memory, disk ve network gibi parametreler için anlık veya geçmişe doğru izlenebilmeli, rapor alınabilmelidir.
    13. Teklif edilen sanallaştırma yazılımı sanal sunuculara VLAN atanmasına izin vermelidir.
    14. Teklif edilen sanallaştırma yazılımı sanal sunucuların açıkken bir kopyasının çıkarılmasına izin vermelidir.
    15. 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.
    16. 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.
    17. Teklif edilen sanallaştırma yazılımı içerisinde çalışan Windows ve Linux sanal makinaların yedeklerini disk ortamına alan bir modülü bulunmalıdır. Bu modül yedeklenmiş verileri tekilleştirme yaparak saklayabilmelidir.
    18. Teklif edilen sanallaştırma yazılımı belirlenen sanal makinaların aynı lokasyondaki veya uzak bir lokasyondaki sanallaştırma sunucuları üzerine replikasyon yapmasına olanak tanımalıdır.
    19. Teklif edilen sanallaştırma yazılımı üçüncü parti antivirus çözümleri ile entegre çalışabilmeli ve ajansız mimari kullanarak sanal makinalar üzerinde virüs taraması yapılmasına olanak sağlamalıdır.
    20. Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinaları diskleri ile birlikte depolama alanları arasında taşıyabilmelidir.
    21. Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinalara CPU, memory, disk ve network kartı eklenmesini desteklemelidir.
    22. 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.
    23. Teklif edilen çözüme ait lisanslar ile birlikte en az 1 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 1 yıl boyunca 7 gün 24 saat üretici destek hizmeti olmalıdır.
    24. Sistem yönetim personeli ilgili yazılımın üreticisine herhangi bir aracıya ihtiyaç duymadan doğrudan çağrı açabilmeli ve doğrudan destek alabilmelidir.

# **Network Sanallaştırma Yazılımı**

* + 1. Network sanallaştırma yazılımı, kurumun yapısında bulunan toplamda 4CPU’yu lisanslayacak şekilde konumlandırılmalıdır.
    2. Network sanallaştırma yazılımı kurumun ihtiyaçları doğrultusunda VMWare NSX DC Advanced Edition olmalıdır.
    3. Network Sanallaştırma yazılımını verecek yüklenici de en az 6(altı) adet Network Virtualization VCP sertifikasına sahip personel çalışmalıdır.
    4. Network Sanallaştırma yazılımını verecek yüklenici Master Services Competency Data Center Virtualization yetkinliğine sahip olmalıdır.
    5. Teklif edilen çözüme ait lisanslar ile birlikte en az 1 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 1 yıl boyunca 7 gün 24 saat üretici destek hizmeti olmalıdır.

# **Ağ Analiz Yazılımı**

* + 1. Veri merkezindeki sanal sunucuların kendi arasındaki ve sanal sunucular ile fiziksel sunucular arasındaki trafiği vSphere Distributed Switch üzerinden IPFIX veya Netflow protokolü ile temin ederek bu trafiğin raporlamasını yapmalıdır.
    2. Yazılım, kurumun yapısında bulunan toplamda 4CPU’yu lisanslayacak şekilde konumlandırılmalıdır.
    3. Raporlanan trafiğe göre güvenlik duvarı kuralı konfigürasyon tavsiyesinde bulunmalıdır.
    4. Raporlanan trafiğin yönlendirilen, anahtarlanan ve internete yönünde olan kısımlarını yüzdesel olarak göstermelidir.
    5. Veri merkezi içerisindeki trafiğin hangi kaynak ve hedef noktalar arasında olduğunu sanal makine başına, vCenter klasörü başına ve ESX Cluster başına göstermelidir.
    6. Ağ sanallaştırma yazılımı ile tam entegrasyonu olmalı ve ağ sanallaştırma yazılımı içerisindeki bileşenleri izleyebilmelidir.
    7. Ağ sanallaştırma yapısındaki bileşenlere ait konfigürasyon hatalarını ve eksikliklerini göstermelidir.
    8. Çoklu üretici desteğine sahip olmalı, desteklenen üreticilerden API, SNMP, SSH gibi yöntemlerin tümü ya da üçüncü üreticinin desteklediği bu herhangi yöntem kullanarak veri toplayabilmelidir.
    9. Olası sorunları raporlayabilmeli, hata ayıklama açısından öneriler sunabilmelidir.
    10. Yazılımın envanterinde bulunan ortama dair bilgileri en az 45 güne kadar saklayabilmeli, hata analizi için geçmişe dönük raporlama sunabilmelidir.
    11. Teklif edilen çözüme ait lisanslar ile birlikte en az 1 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 1 yıl boyunca 7 gün 24 saat üretici destek hizmeti olmalıdır.

# **Operasyon Yönetimi Yazılımı**

* + 1. Yazılım 4 çekirdek (cpu) için lisanslanacaktır
    2. Yazılım özelliklerinde Kullanıma Hazır Gösterge Tabloları, Görünümler, Raporlar, Isı Haritası, Performans Grafikleri gibi özellikler mevcut olmalıdır
    3. Performans İzleme ve Analitik olarak vSphere Güvenliği ve Uyumluluğu (DISA, FISMA, ISO, CIS, PCI ve HIPAA) olmalıdır
    4. Gerçek Zamanlı Tahmine Dayalı Kapasite Yönetimi: Trend Oluşturma, Ölçüm, Doğru Boyutlandırma, Optimizasyon özelliklerini barındırmalıdır.
    5. Sanal Makinelerin Eklenmesi / Kaldırılmasına Yönelik What-If Senaryoları yapılabilmelidir
    6. Manuel İş Yükü Optimizasyonu , Tahmine dayalı DRS ve DRS Yönetimi , Kılavuzlu İyileştirme, vSAN Genel Bakış ve Geçiş Gösterge Tabloları, vRealize Log Insight Entegrasyonu olmalıdır.
    7. VMware ve Üçüncü Taraf Altyapı Yönetiminde Dell EMC Depolama’yı desteklemelidir.
    8. Yazılım 1 yıl 7x24 üretici supportuna sahip olmalıdır.

# **Veri Yedekleme Yazılımı**

* + 1. Yazılım Vmware vSphere (4.1, 5.x ve 6.x) ve Microsoft Hyper-V (2008R2, 2012, 2012R2, 2016) sanallaştırma platformlarında çalışan sanal makinaların yedeklemesini ve replikasyonunu herhangi bir ajan kurulumu gerektirmeden, imaj seviyesinde ve uygulama tutarlı olarak yapabilmelidir.
    2. Yazılım, yedekleri saklamak için Windows, Linux, CIFS/SMB dosya paylaşımlarını ve üzerinde dahili tekilleştirme sunan cihazları kullanabilmelidir.
    3. Yazılım HPe ve DellEMC tekilleştirme ünitelerinin lisanslı (Boost ve Catalyst) eklentileri ile entegre çalışabilmeli ve tekilleştirmenin bir kısmını kaynakta yaparak ağ üzerinden geçen trafiği ve diskteki yükü azaltmalı ve yedekleme sürelerini kısaltmalıdır.
    4. Yazılım tanımlanmış sınırsız sayıda yedekleme deposunu tek bir ‘büyütülebilen yedek deposu’ olarak kullanarak disk alanı yönetimini basitleştirmelidir.
    5. Yazılım 4 CPU için lisanslanmalıdır.
    6. Yazılım bir yedekleme görevi içindeki her sanal makina için ayrı ayrı tam ve artımlı dosya zincirleri oluşturabilmelidir.
    7. Yazılım herhangi bir ajan kurulumu gerektirmeden kullanıcı tarafından özelleştirilebilen veya devre dışı bırakılabilen dahili sıkıştırma ve tekilleştirme sunmalıdır.
    8. Yazılım artımlı yedekler için hipervizörlerin sunduğu Değişen Blok Takibi (CBT) özelliğini kullanmalıdır.
    9. Yazılım yedeklerin saklandığı diskte bulunan tam ve artımlı yedekleri kullanarak yeni tam yedekler oluşturabilmelidir.
    10. Yazılım ile yedeklenmesi istenmeyen sanal diskler ile NTFS dosya sistemlerindeki dosya ve klasörler seçilerek; geçici dosyalar ve silinmiş öğelere ait disk blokları tespit edilerek yedekleme ve replikasyon işlemi dışında bırakılabilmelidir.
    11. Yazılım yedekleme ve replikasyon için sanal makina verisini doğrudan Veri Depolama ağı üzerinden, Ağ üzerinden veya Hipervizör I/O platformu üzerinden aktarma seçenekleri sunmalıdır.
    12. Yazılım NFS disk alanlarına direkt erişerek yedekleme, replikasyon ve kurtarma işlerini hızlandıracak Vmware NFS 3 ve 4.1 destekli bir istemci sunmalıdır.
    13. Yazılım saklanan yedekleri ve ağ trafiğini uçtan uca (kaynakta, aktarırken ve depolarken) AES256bit şifreleyebilmeli ve kayıp şifre koruması sunmalıdır.
    14. Yazılım diskte bulunan yedekleri replikasyon kaynağı olarak kullanarak geri dönüş noktalarını yedeklerden oluşturabilmelidir.
    15. Yazılım görevlerin kullanabileceği network bant genişliğini, eş zamanlı çalışacak görev sayısını, backup diskine aynı anda yazılabilecek kanal sayısı ve veri oranını yöneticinin istediği değerlerde limitleyebilmelidir.
    16. Yazılım kaynak Sanal Makinaların bulunduğu disk alanılarındaki I/O gecikmelerini izleyebilmeli ve kullanıcı tarafından belirtilen değer aşıldığında o disk alanı üzerinde bir yedekleme veya replikasyon görevi başlatmamalı ve çalışan ortam performansının olumsuz etkilenmesi engellenmelidir. I/O gecikmesi eşik değerleri her bir disk alanı (datastore) için farklı olarak ayarlanabilmelidir.
    17. Yazılım bir disk alanına alınmış yedeklerin tamamını veya sadece içerisinden seçilen belirli Sanal Makinaların yedeklerini ikincil bir disk alanına; yedeğin kopyalanması veya uzun dönem arşivlenmesi (GFS) amacı ile otomatik olarak kopyalayabilmeli, periyodik doğrulama ve hata giderme yapabilmelidir.
    18. Yazılım bir disk alanına alınmış yedekleri ve Windows veya Linux sunucular içerisinden dosyaları teyp ünitelerine, teyp kütüphanelerine ve Sanal Teyp Kütüphanelerine arşivleyebilmeli, teyp üzerindeki dosya ve yedek dönüş noktalarının takibini yapabilmelidir.
    19. Yazılım teyp medya havuzlarının birden fazla teyp kütüphanesi üzerinde oluşturulabilmesini, teypleri paralel kullanabilmeyi ve teyp havuzları üzerinde GFS arşivlemeyi desteklemelidir.
    20. Yazılım teybe yedeklenmiş bir sanal makinanın doğrudan ana sunucu üzerine geri yüklenmesini desteklemelidir.
    21. Yazılım üretici onaylı bir bulut servis sağlayıcı tarafından sunulan Bulut üzerinde disk hizmetini, yedeklerin saklanacağı bir yedek deposu olarak tanımlayabilmeli, yedeklerini veya yedek kopyalarını bu alana gönderebilmelidir.
    22. Yazılım üretici onaylı bir bulut servis sağlayıcı tarafından sunulan Bulut üzerinde Sanal Ana Sunucu hizmetini, replikasyon hedef ana sunucusu olarak tanımlayabilmeli ve sanal makina replikasyonu yapabilmelidir.
    23. Yazılım daha az ağ bant genişliği kullanarak yedekleri ikinci bir disk alanına kopyalamak veya sanal makina replikasyonu yapabilmek için dahili WAN Hızlandırıcı sunmalıdır.
    24. Yazılım Microsoft SQL ve Oracle sunucuların içerisinden ajan kullanmadan belirtilen disk alanına ve yedekleme görevinin zamanlama ayarlarından bağımsız frekanslarda ‘Transaction Log’ yedeği alabilmelidir.
    25. Yazılım HP 3PAR StoreServ, HP StoreVirtual, HP StoreVirtual VSA, NetApp Data ONTAP tabanlı NetApp FAS, NetApp FlexArray (V-Serisi), NetAppData ONTAP Edge, IBM N Serisi, DellEMC VNX, VNX2,VNXe, UNITY ve NimbleStorage AF ve CS Serisi Veri Depolama ünitelerinin desteklenen bağlantı ve protokolleri üzerinde,
    26. Oluşturduğu Donanımsal Snapshot’ları kullarak Yedekleme ve Replikasyon kaynağı olarak kullanabilmeli,
    27. Oluşturduğu veya daha önce oluşturulmuş Donanımsal Snapshot’lar içerisinden komple Sanal Makina, hipervizör tarafından desteklenen tüm işletim sistemlerinden dosya ve uygulama öğesi (Microsoft Exchange, Active Directory, SharePoint, SQL öğeleri ve Oracle veri tabanları) kurtarabilmelidir.
    28. Oluşturduğu veya daha önce oluşturulmuş Donanımsal Snapshot’lar içerisinden Sanal Makinaları izole ortamda açarak üretim ortamının bir kopyasını oluşturabilmelidir.
    29. Yazılım yedekleme yaparken desteklenen NetApp ve NimbleStorage birincil depolama üniteleri üzerinde oluşturduğu uygulama tutarlı donanımsal Snapshot’ların bir kopyasını aynı markaların ikincil depolama üniteleri üzerinde oluşturabilmeli ve bu kopyaları da yedekleme ve replikasyon kaynağı olarak kullanabilmelidir.
    30. Yazılım diske alınan her yedeği otomatik olarak doğrudan yedek dosyasından izole bir ortamda çalışır hale getirerek, işletim sistemi, hipervizör servisi ve uygulama seviyesinde test ederek bunu rapor olarak ilgili kullanıcılara gönderebilmelidir.
    31. Yazılım her bir replikasyon kurtarma noktasını otomatik olarak doğrudan replike edilmiş sanal makinayı izole bir ortamda çalışır hale getirerek, işletim sistemi, hipervizör servisi ve uygulama seviyesinde test ederek bunu rapor olarak ilgili kullanıcılara gönderebilmelidir.
    32. Yazılım bir veya birden fazla Sanal Makinayı doğrudan yedek dosyasından veya replikasyon noktasından, izole bir ortamda kullanıcının belirleyeceği sıra ve kaynak ile çalışır hale getirerek test, hata tespiti veya eğitim amaçlı kullanılmasını sağlamalıdır.
    33. Yazılım replike edilmiş bir Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış Sanal Ağ ayarları ile çalışır duruma getirebilmelidir.
    34. Yazılım replike edilmiş Microsoft Windows işletim sistemine sahip bir Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış IP ayarları ile çalışır duruma getirebilmelidir.
    35. Yazılım veri kaybı olmadan veri merkezi taşımasını organize edecek Planlı Taşıma özelliği sunmalıdır.
    36. Yazılım bir veri merkezi kesintisi sırasında tek tuşla tüm sanal makinaları tanımlanan sırayla çalışır hale getirebilecek bir Kurtarma Planı hazırlama özelliği sunmalıdır.
    37. Yazılım bir sanal makinayı doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilmelidir.
    38. Yazılım bir sanal makinayı tam veya artımlı yedek dosyasından orjinal yerine veya başka bir ana sunucu üzerine geri yükleyebilmelidir.
    39. Yazılım bir sanal makinayı yedekten geri yüklerken sadece değişen blokları kullanarak kurtarma yapabilmelidir.
    40. Yazılım bir sanal makinanın sadece ana sunucu üzerindeki dosyalarını geri yükleyebilmelidir.
    41. Yazılım bir sanal makinanın sadece seçilen sanal disklerini geri yükleyebilmelidir.
    42. Yazılım geçerli bulut hizmetleri abonelik bilgileri sağlandığında, bir sanal makinayı doğrudan Microsoft Azure ortamına geri yükleyebilmelidir.
    43. Yazılım sanal makinaya herhangi bir ajan/servis kurulumu gerektirmeden, sanallaştırma platformunun desteklediği tüm işletim sistemlerinden, sunucunun tamamını geri yüklemeye gerek kalmadan sadece istenilen klasör veya dosyaları arama, bulma, dışa aktarma ve geri yüklemesini yapabilmelidir.
    44. Yazılım sunucuya bir ajan/servis kurulumu gerektirmeden, Microsoft Active Directory, Microsoft Exchange, Microsoft SQL, Microsoft Sharepoint ve Oracle yedekleri içerisinden uygulama öğelerini ve veri tabanlarını orjinal yerine geri yükleyebilmeli veya dışarı aktarabilmeli, bu işlemi yedeklerden, replikalardan ve yedek kopyalarından gerçekleştirebilmelidir.
    45. Yazılım PostgreSQL, MySQL dahil her türlü sanallaştırılmış uygulamadan uygulamaların yönetim araçlarını kullanarak obje bazlı kurtarma yapabilmek için sanal makinayı doğrudan yedek dosyasından veya replikasyon noktasından izole bir ortamda açarak kullanıcı erişimine sunabilmelidir.
    46. Yazılımın Web uygulaması kullanılarak Sanal Makinaların, dosyaların, SQL Veri tabanlarının ve Exchange Posta kutularının geri yüklemesi yapılabilmeli, kişi ve gruplara geri dönüş yetkilendirmesi verilebilmelidir.
    47. Yazılım vSphere Web Client’a entegre olabilmeli, anlık hızlı yedeklemeler buradan başlatılabilmeli, yedeklerin ve yedekleme kaynaklarının durumları, yedeklerin saklandığı disklerin boş/dolu alan bilgileri, korunan sanal makinalar gibi bilgilere doğrudan web client içerisinden erişilebilmelidir.
    48. Yazılım Vmware vCloud Director yapısı üzerinden Sanal Makina, vApp ve metadata’ları doğrudan yedekleyebilmeli ve aynı bileşenleri orjinal yerlerine ya da farklı bir vCloud Director yapısı üzerine geri yükleyebilmelidir.
    49. 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.
    50. Yazılım kendi konfigurasyon yedeğini herhangi bir kullanıcı müdahalesi gerekmeden tanımlı disk alanına alabilmeli ve tüm ayarları ve tanımlamaları içerecek şekilde geri yüklenebilmelidir.
    51. Uzak ofislerde ve uç noktalarda yedekleme ve kurtarma işlemleri için uzak nokta etkileşim proksi sunucusu ve yükleme sunucuları kullanılabilmelidir.
    52. Yazılım dahili komut satırı (PowerShell) Desteği sunmalıdır.
    53. Yazılım, uygulama geliştiriclerin http ve https protokolleri ile yazılıma bağlantı kurarak bilgi alabilecekleri ve REST prensiplerini kullanan bir programlama arayüzü (API) sunmalıdır.
    54. Yazılımın yönetim konsolu 64 bit bir Microsoft Windows işletim sistemine sahip herhangi bir fiziksel veya sanal, sunucu veya kişisel bilgisayar üzerinde, çoklu kullanıcı ve sunucu/istemci modeli ile çalışmalıdır.
    55. Yazılımın tüm bileşenleri Microsoft Windows Server 2016 üzerine kurulabilmeli ve tüm özellikleriyle desteklenmelidir.
    56. Yazılım yeni versiyon ve güncellemeleri yayınlandığında konsolda uyarıda bulunmalı ve yöneticiyi ilgili indirme sayfasına yönlendirmelidir.
    57. Yazılımın lisanslaması korunmakta (yedeklenmekte ve/veya replike edilmekte) olan sanal makinaları çalıştıran ana sunucuların fiziksel işlemcisi bazında olmalıdır. Yapısal bilşenlerin sayısı (proksi, konsol, disk vb), işlemci çekirdeği, Sanal Makina sayısı, disk kapasiteleri ve uygulama ajanlarına göre bir lisanslama modeli olmamalıdır.
    58. Lisanslama modelinde bir üst limit bulunmamalı, ilave lisans alınarak yapı istenildiği kadar sunucuyu kapsayacak şekilde büyütülebilmelidir.
    59. Teklif edilen çözüme ait lisanslar ile birlikte en az 1 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 1 yıl boyunca 7 gün 24 saat destek hizmeti verilmelidir.
  1. **TOR SWİTCH TEKNİK GEREKSİNİMLERİ (2 ADET)**
     1. Anahtar uzerinde en az 24 adet 25GbE SFP+ ve en az 4 adet 100GbE QSFP28 fiber yuva bulunmalidir.
     2. Hiperbütünleşik sistem network bağlantıları için 2 adet TOR switch konumlandırılacaktır.
     3. Anahtarin Switching kapasitesi en az 2 Tbps full-duplex olmalidir.
     4. Teklif edilecek switche 8 adet en az 3m SFP28 to SFP28, 25GbE bakır DAC kablo eklenecektir.
     5. Teklif edilecek switche 2 adet 100GbE QSFP2 Transceiver eklenecektir
     6. Anahtarin yonlendirme kapasitesi en az 900 Mpps olmalidir.
     7. Anahtarin Packet Buffer kapasitesi en az 16 MB olmalidir.
     8. Anahtarin CPU hafizasi en az 16GB olmalidir.
     9. Anahtar en az 64000 MAC adres kaydini desteklemelidir.
     10. Birbirine bagli iki adet anahtarin aktif-aktif yedekli calismasini saglayan VSS, VPC, IRF veya VLT ozelliklerinden en az birisi desteklenmelidir.
     11. Anahtar MSTP ve RSTP spanning tree protokollerini desteklemeli ve RPVST+ protokolu ile uyumlu calisabilmelidir.
     12. Anahtar Enhanced Transmission Selection (802.1Qaz), Priority Flow Control (802.1Qbb), DCBx ozelliklerini desteklemelidir
     13. Anahtar en az 128000 adet IPv4 veya 64000 adet IPv6 yonlendirme kaydi desteklemelidir.
     14. Anahtar IGMPv1,v2,v3 ve MLD v1,v2 snooping multicast protokollerini desteklemelidir.
     15. Anahtar SNMPv1,v2 ve v3 protokollerini desteklemelidir.
     16. Anahtar Sflow veya netflow özelligini desteklemelidir.
     17. Anahtar 802.1x ozelligini desteklemelidir.
     18. Anahtar Radius, Tacacs+ ve SSHv2 protokollerini desteklemelidir.
     19. Anahtar VXLAN desteklemelidir.
     20. Anahtar guc kaynagi ve ve fanlari hot-swap ve yedekli olmalidir ve bu komponentler yedekli olarak teklif edilmelidir.
     21. Anahtar en az 3 yil geçerli, 7 x24 üretici destek merkezine erişim sağlayabilen, ertesi iş günü yerinde müdahale içeren üretici destek paketi ile teklif edilmelidir. Bu destek partner bağımsız üreticinin destek paketi olmalıdır.

1. **GÜVENLİK TEKNİK ŞARTNAMESİ**
   1. **AĞ GÜVENLİK CİHAZI ( 2 Adet )**
      1. Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.
      2. Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;
      3. Güvenlik Duvarı (Firewall)
      4. IPSec VPN Sonlandırma Sistemi
      5. SSL VPN Sonlandırma Sistemi
      6. Saldırı Tespit ve Engelleme Sistemi (IPS)
      7. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
      8. Virüs/Zararlı İçerik Kontrolü
      9. URL Kategori Filtreleme
      10. Bant genişliği yönetimi
      11. Özelliklerine sahip olmalıdır.
      12. Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlamalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.
      13. Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, herhalukarda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.
      14. Teklif edilen Ağ Güvenlik Duvarı High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.
      15. Yedeklilik konfügrasyonunda her segment için güvenlik duvarı üzerinde set edilecek Ip sayısı 1 (bir) adet olmalıdır. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.
      16. Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.
      17. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır
      18. Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN’lar arayüz (interface) olarak kullanılabilmelidir.
      19. Sistem Sanal Güvenlik Duvarı özelliği ile kullanıldığı durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilmelidir.
      20. Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.
      21. Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
      22. SPI (stateful packet inspection),
      23. Saldırı Tespit ve Engelleme Sistemi (IPS)
      24. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
      25. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
      26. URL Kategori Filtreleme
      27. Routing modda aşağıdaki özellikleri sağlamalıdır;
      28. SPI (stateful packet inspection),
      29. IPSec VPN Sonlandırma,
      30. SSL VPN Sonlandırma,
      31. Saldırı Tespit ve Engelleme Sistemi (IPS)
      32. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
      33. Virüs/Zararlı İçerik Kontrolü
      34. URL Kategori Filtreleme
      35. Bant genişliği kontrolü
      36. Statik yönlendirme (static routing),
      37. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
      38. Sunucu yük dengeleme
      39. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.
      40. Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.
      41. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.
      42. Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.
      43. Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.
      44. Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
      45. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
      46. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
      47. Uygulama bazında bant genişliği kontrolü yapabilmelidir.
      48. Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.
      49. 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.
      50. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.
      51. Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.
      52. IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilmelidir.
      53. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.
      54. Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.
      55. 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.
      56. SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.
      57. SSL VPN özelliği eşzamanlı minimum 5.000 kullanıcı lisansı ile teklif edilecektir.
      58. 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.
      59. SSL VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, Bant Genişliği yönetimi (QoS) özellikleri uygulanabilir olmalıdır.
      60. Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3 trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment’leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir
      61. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.
      62. 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.
      63. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı URL filtreleme politikaları set edilebilmelidir.
      64. Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.
      65. Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.
      66. Çözüm sıfır-gün ataklarına karşı, bulut tehdit engelleme sistemleri ile entegre olmalı, bu sayede koruma seviyesini arttırmalı ve potansiyel hatalı tespit sayılarını azaltabilmelidir. Sıfır-gün ataklarına karşı koruma sağlamak için, Firewall’lar üzerine eklenebilecek bulut tehdit engelleme sistemleri lisansları 1 yıl geçerli olacak şekilde teklif edilmelidir.
      67. 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.
      68. İstenildiğinde categorilerden bağımsız olarak, sisteme eklenebilecek tam URL bilgisi (Örneğin: [www.abc.com/deneme/sayfa1.php](http://www.abc.com/deneme/sayfa1.php)) bazında engelleme yapabilmelidir.
      69. SSL trafiğini kendi üzerinde yaratılan bir sertifikayı yada farklı bir CA den alınmış yeterli özelliklere sahip bir sertifika ile inceleyebilmelidir. Bu sayede sadece domain bazında değil, URL bazında (Örneğin: [www.abc.com/deneme](http://www.abc.com/deneme)/test.php) engelleme yapabilmelidir. URL kategorileri bazında SSL incelemeye girmeyecek domainler belirlenebilmelidir.
      70. URL filtreleme uyarı ekranları özelleştirilebilecektir.
      71. 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.
      72. Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
      73. Seri bağlantı ile konsol port üzerinden,
      74. Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
      75. SSH bağlantı ile komut satırı (commandline) üzerinden
      76. Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir
      77. Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.
      78. Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.
      79. Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, “NSS Labs Network IPS” ve “NSS Labs Next Generation Firewall” testlerine girmiş olması gereklidir.
      80. Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel “Enterprise Firewall” için “Gartner Magic Quadrant” tablosunda “Leaders” kısmında yer almalıdır.
      81. Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.
      82. Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.
      83. Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.
      84. SSL bağlantıları için SSL Offloading özelliği olmalıdır.
      85. Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:
      86. Kaynak Ip hash bilgisi
      87. Round robin
      88. Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak
      89. Aktif durumda olan gerçek sunuculardan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi
      90. Ping paketlerine verilen cevaplar esas alınması
      91. Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak
      92. Wan optimizasyon özelliklerine sahip olacaktır.
      93. Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.

# **Güvenlik Duvarı Performans Değerleri**

* + 1. Teklif edilen Ağ Güvenlik Duvarı, yedekli çalıştırılacak şekilde 2 adet teklif edilecektir ve şartnamede belirtilmiş tüm güvenlik servis lisansları (IPS, URLFilter, App Control, VPN) her iki cihaz içinde teklife dahil edilecektir.
    2. Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, en az 36 Gbps Firewall performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
    3. Her bir Ağ Güvenlik Duvarı ünitesi (cluster içerisindeki herbir cihaz ayrı ayrı olmak üzere) Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az 7 Gbps kapasiteye sahip olmalıdır. Bu kapasite kullanıcı/istemci arasındaki istek-cevap trafiğinin toplamına (çift yönlü analiz ile) bu güvenlik özelliklerinin uygulandığı konfigürasyonda belirlenmiş olmalıdır. Belirtilen bu değer ürün kataloglarında yer almalıdır. Ürün kataloglarında Tehdit Koruma için farklı terminoloji kullanılmış ise bu koşulda ürün kataloğunda NGFW (Firewall + IPS + Uygulama Denetimi) kapasitesi gerçek ortam değeri baz alınarak en az 9.5 Gbps olmalıdır.
    4. Sistem aynı anda en az 8 milyon oturumu desteklemeli ve saniyede en az 450.000 yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
    5. Güvenlik Duvarı Sistemi en az 20 Gbps IPSec VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
    6. Güvenlik Duvarı Sistemi en az 7.0 Gbps SSL VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
    7. Sistem Site-to-Site için en az 2.000 adet, Client to site için 10.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir
    8. Sistem en az 10 Gbps IPS throughput performans değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
    9. Sistem üzerinde; En az 8 adet 1GE RJ45 ara yüz bulunmalıdır.
    10. En az 8 adet 1GE SFP ara yüz bulunmalıdır.
    11. En az 2 adet 10GE SFP+ ara yüz bulunmalıdır.
    12. Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama Sistemine kayıt gönderebilmelidir.
    13. Sistemin; Firewall, IPS fonksiyonlarının hiçbiri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 1 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 1 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.
  1. **AĞ GÜVENLİK CİHAZI MERKEZİ YÖNETİM , LOGLAMA VE RAPORLAMA MODÜLÜ**

**Merkezi Yönetim Sistemi**

* + 1. Yönetim ve Raporlama yazılımı teklif edilen donanımsal ve Yeni Nesil Sanal Güvenlik duvarlarının yönetimini, loglamasını ve raporlamasını merkezi olarak yapacaktır.
    2. Çözüm ile hem merkezdeki hemde şubelerdeki cihazları merkezi olarak yönetilebilecektir.
    3. Çözüm sanal veya fiziksel appliance olarak teklif edilebilir.
    4. Çözüm en az 10 adet cihazı yönetebilecek şekilde tekliflendirilecektir.
    5. Merkezi yönetim çözümü ile yönetilen cihazlardaki bütün konfigürasyon objeleri tanımlanabilecek ve ilgili politikalar merkezi olarak oluşturulup cihazlara uygulanabilecektir.
    6. Merkezi yönetim çözümü ile beraber, yerel veya uzakta bulunan firewall veya accespoint cihazların otomatik olarak devreye alınması için gerekli “Zero Touch Provisioning” lisansı verilmelidir.
    7. Merkezi yönetim çözümü cihazların üzerindeki konfigleri çekebilecektir.
    8. Merkezi yönetim çözümünün cihazlar arasındaki VPN bağlantılarının merkezi konfigürasyonunun yapılmasına ve monitor edilmesini yarayan bir modulu olmalıdır.
    9. Merkezi yönetim çözümü üzerinde hiçbir ayar olmayan cihazların kendisine ulaşamasına ve daha önceden belirlenmiş şablonlara göre konfigürasyon basılmasını (Zero Touch Provisioning) destekleyecektir.
    10. Merkezi Yönetim yazılımı çok sahiplilik desteği ile bir den çok gruba farklı yetkilerle hizmet edebilmelidir (Multi-Tenancy)
    11. Merkezi yönetim yazılımı yeni politikaların uygulanaması yada olan politikalarda değişiklik yapılması sürecinin gözden geçirilmesini, onaya tabi olmasını ve audit edilmesini destekleyecektir.
    12. Merkezi Yönetim yazılımı üzerinde merkezi imza veritabanı oluşturulabilir ve her bir cihazın internet üzerinden ayrı ayrı imza ve diğer güncel güvenlik verilerini çekmesi yerine merkezi olarak kendi üzerinden çekilmesini desteklemelidir.
    13. Merkezi yönetim yazılımı restful API ile harici uygulamalar ile entegre olabilecektir.Bu sayede harici sistemler merkezdeki ve şubelerdeki cihazlardan API aracılığı ile veri çekebilecekler ve konfigürasyon değişikliklerini gerçekleştirebileceklerdir.
    14. Yukarıda belirtilen seçeneklerden hangisi ile teklif edilirse edilsin, teklif edilen sistemlerin en az 1 yıl yazılım garantisi bulunmalıdır. 1 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

**Loglama ve Raporlama Modülü**

* + 1. Önerilen güvenlik duvarı sisteminin kayıt depolama ve takibini, raporlama işlemlerini gerçekleştirmek için aşağıda belirtilen şartlara uyan kayıt takip ve raporlama ürün/ürünleri alınacaktır.
    2. Aşağıda belirtilen özellikler yönetim ve kayıt sistemlerinin ayrı veya tek bir sistem olarak önerilmesi durumunda da sağlanacaktır.
    3. Önerilen sistem, saniyede en az 6 GB/Gün log kayıt alabilmelidir.
    4. Log kayıt alanı olarak en az 3 TB depolama alanını desteklemelidir.
    5. Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.
    6. Cihaz üzerinden geçen tüm trafiğin günlüklerde tutulması, istenen kıstaslara göre (En az IP, IP aralığı, ağ, protokol, zaman) filtrelenebilmesi ve aktif bağlantıların gerçek zamanlı izlenebilmesi sağlanacaktır.
    7. Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.
    8. Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilmelidir.
    9. Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.
    10. Merkezi yönetim dâhilinde bulunan bileşenlere ait anlık ortalama CPU, boş disk alanı, firewall, firewall cluster üzerinden akan tüm uygulamalar, kullanıcı IP adresleri ve dâhili kullanıcı isimleri gibi değerler anlık ve sürekli olarak görüntülenebilecektir.
    11. Önerilen kayıt yönetim sistemi geçmişe yönelik olarak raporlama yapabilme özelliğine sahip olacaktır. Örneğin bant genişliği kullanımı, uygulama denetimi, URL filtreleme ile ilgili istenen tarih aralıklarında raporlar üretebilecektir.
    12. Tutulan kayıt alanları baz alınarak özelleştirilmiş sorgular yazılabilmeli ve bu sorguların çıktıları, tablo, pie-chart şeklinde raporlar içerisine konulabilmelidir.
    13. pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.
    14. Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek kayıtların yedekliliği sağlayabilmelidir.
    15. Yukarıda belirtilen seçeneklerden hangisi ile teklif edilirse edilsin, teklif edilen sistemlerin en az 1 yıl yazılım garantisi bulunmalıdır. 1 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.
  1. **LOG YÖNETİM CİHAZI**
     1. Yönetim, log toplama, ham log kaydetme modülleri fiziksel olarak sunulmalı, tek ekrandan yönetilmelidir.
     2. Sunulacak mimari yönetim, log toplama, ham log kaydetme modülleri için en az 5000 EPS değerinde hizmet verecek şekilde planlanmalıdır.
     3. SIEM çözümünde teklifin verildiği tarih itibarı ile ileride üreticiye ait sonradan satın alınabilecek uygulama ve veri tabanı aktivitelerini denetleyen modüllerin bulunması tercih sebebi olacaktır.
     4. Önerilen sistem gerçek zamanlı olarak korelasyon, benzer olayları aynı imza, aynı kaynak ve hedef IP doğrultusunda birleştirebilmeli ve bunun için ayrı bir ürüne ihtiyaç duymamalıdır. Olayları ait aktiviteleri tek tek RAW log biçiminde saklayabilmelidir.
     5. Tek bir klik ile orijinal log dosyasına ve raw log verilerine ulaşılabilmelidir. Tek bir GUI ile korelasyon, log ve olay araştırması, custom parser, raporlama imkanı sağlanmalıdır.
     6. Sisteme ait yönetim modülü alt modüllerin merkezi olarak tek noktadan yönetimine imkan tanımalıdır (Security Manager, Log Manager , Receiver, Reputation feed, reporting, creations of custom parsers..)
     7. Canlı ve tarihsel verilere ulaşım için kendisine ait native veri tabanı kullanılmalı bu amaçla 3’ncü parti veri tabanı (SQL temelli) ürünleri kullanılmamalıdır.
     8. Hızlı analitik araştırmalar için tüm index’ler primary memory ’de saklanabilmelidir.
     9. Sistem yöneticisi, olaylara istinaden oluşan temel eşiklerin (Baselining) aşılması durumlarından haberdar edilebilmelidir.(uyarı gibi yöntemlerle) Bu eşikler otomatik olarak düzenli sistem tarafından oluşturulmalıdır. Baselining ile monitör edilen tüm aktiviteler, ağ kullanıcıları uygulamalara ait anomaliler ve tarihsel veriler üzerinde farkların incelenmesi mümkün olmalıdır.
     10. Korelasyon kuralları için kolay kullanılan ve öğrenilen GUI sağlanmalıdır.
     11. En az 260 adet ön tanımlı korelasyon kuralı bulunmalıdır. Bu kurallar güncellemelerle gelişen yapıda olmalı ve aktif olmalıdır.
     12. Sistemin firmware güncellemeleri ve yamaları GUI üzerinden kolayca yapılabilmelidir.
     13. Kural ve Geo Location güncellemeleri gerek internet gerekse manual yapılabilir yapıda olmalıdır.
     14. Yönetim sistemi zone kavramını desteklemeli bu yolla örneğin DMZ bölgesindeki log kaynakları farklı zone altında birleştirilebilmelidir.
     15. Önerilen SIEM GUI si hazır ve amaca özel dashboard ’lar barındırmalı, sistem yöneticisi kolayca yeni dahboard’lar ekleyebilmelidir.
     16. Yönetim ara yüzü üzerinden politikalar yaratılabilmeli, kurallar ve alertler oluşturulabilmeli, bunlara istinaden düzeltme(mitigation) yapılabilmelidir.
     17. Yönetim sistemi herhangi bir ek lisans veya çözüme gerek duymadan iş akışlarını destekleyen olay yönetim ve alarm alt yapısını desteklemelidir.(case management)
     18. Oluşan alarm’lar ayrı bir dashboard üzerinde kolayca izlenebilmeli, filtrelenebilmeli ve içerikleri görülebilmelidir.
     19. Sistem üzerindeki tüm sistem yönetici aktiviteleri (Audit) detaylı şekilde raporlanmalı ve filtrelenebilmelidir.
     20. Merkezi yönetim birimi harici helpdesk yazılımlarına SNMP ve Email üzerinden çağrı kaydı açabilmelidir.
     21. Her bir log kaynağı için ayrı storage pool tanımlanabilmeli bu yolla bu her kaynak için disk üzerinde farklı miktarda bir disk alanı rezerve edilebilmelidir. Bunun için kurum tarafından harici disk alanı sağlanacaktır.
     22. Her bir kayda ait olay tanımlarında, olaya ait atanan severity ve aggregation ayarları el ile değiştirilebilmelidir. Örneğin şu tip bir Windows event’i oluşursa; kayıtlama, aggregation yapma yada severity şu olsun gibi.
     23. Varlıklar üzerinde “String Nomalization” desteklenmelidir. Örneğin belli kalıplarlar tanımlanmış kullanıcı isimleri gerçek kullanıcı isimleri ile map edilebilmeli ve bu bilgiler raporlarda görülebilmelidir.
     24. Yönetim arabirimi zengin(en az 800) ön tanımlı raporlara sahip olmalı sistem yöneticisi el ile kendi raporlarını kolayca oluşturabilmelidir.
     25. Çözüm bağlamsal bilgiye göre olay zenginleştirmeyi desteklemeli bu yolla vulnerability assessment, identity, authentication management systems, privacy solutions gibi çözümlerle entegre olabilmelidir.
     26. SIEM çözümü PCI-DSS, HIPAA, NERC-CIP, FISMA,GLBA, SOX gibi standartları destekleyen hazır rapor şablonlarına sahip olmalı ve ekstra lisans gerektirmemelidir.
     27. Üretici tarafından otomatik ve ücretsiz olarak içerik paketleri sağlanmalı ve bu paketler ile farklı üreticilere ait Firewall ve Web Gateway ürünleri ile ürün bağımsız olarak kimlik doğrulama, Active Directory politikaları, Windows kimlik doğrulama, IPS/AntiVirus olaylarına ait özel içerikler sunulmalı. İçerik paketleri ile monitör, alarm, raporlama, izleme listeleri, değişkenler ve korelasyonlar kuralları otomatik olarak gelmeli.
     28. Merkezi yönetim arabirimi aşağıdaki liste seçeneklerini desteklemelidir:
     29. Statik Liste: Spesifik Kullanıcı, IP adres ve grup. Bu listelere el ile, dosya import yoluyla ya da API ile doldurulabilmelidir.
     30. Dinamik Liste: Regex, Database, Ldap aramaları
     31. Korelasyon kurallarına istinaden otomatik update edilen listeler
     32. Önerilen çözüm üzerinde dinamik listeler ile internet ortamında bulunan kaynaklardan otomatik olarak besleme yapılabilmelidir. Örnek olarak siber tehdit olarak daha önceden belirlenmiş IP adreslerinin otomatik olarak bir listede tutulmalı, liste güncellenmeli ve bu liste kullanılarak riskli aktiviteler tespit edilerek alarm üretilmeli, raporlanabilmeli. Güncelleme işlemleri otomatik olmalı ve MITRE Threat Information Exchange (TAXII) ve benzeri otoriteler desteklenmeli.
     33. Önerilen çözüm ile loglar üzerinde ilgili alanlardaki bilgiler internet ortamında bulunan kaynaklardan kolayca çağırılarak sorgulanabilmeli. Örnek olarak Firewall loglarında yer alan IP adreslerinin DShield.org, MXToolBox.com, Robtex.com, TrustedSource ve benzeri sitelerden otomatik olarak çağırılabilmeli.
     34. Önerilen çözüm aynı markaya ait antivirus, Network IPS ile entegre çalışarak olası risk senaryolarında bu güvenlik sistemleri üzerinde aksiyon alarak risk’i engelleyebilmelidir.
     35. Korelasyon kurallarına istinaden e-mail, görsel, sms gibi yöntemlerle uyarı oluşturulabilmelidir.
     36. En az 2 farklı korelasyon kuralı birleştirilerek tek bir sonuç üretilebilmelidir.
     37. SIEM appliance’lar en az FIPS 140-2 level 2 seviyesinde sertifikalara sahip olmalıdır.
     38. Olaylar üzerinden Geo Location bilgileri ile ülke raporları alınabilmelidir.
     39. Receiver modülü en az aşağıdaki tipteki cihazlardan log alabilmelidir:
     40. Identity and authentication Systems
     41. Firewalls
     42. Vulnerability Scanner
     43. Physical Security Devices
     44. IDS/IPS devices
     45. UTMs
     46. Switches
     47. Routers
     48. Applications
     49. Servers and workstations
     50. En az aşağıdaki yöntemlerle log alabilmelidir:
     51. Ftp
     52. Syslog
     53. Cifs
     54. Nfs
     55. OPSEC
     56. ODBC
     57. WMI
     58. Ajan yöntemi
     59. Snmp trap
     60. Flow
     61. HTTP
     62. Bilinmeyen ve desteklenmeyen log tipleri için SDK veya ek lisansa gerek kalmadan custom parser yazma imkanı sağlanmalıdır.
     63. Custom Parser için ek GUI ye gerek kalmamalıdır.
     64. Sistemden PDF, HTML ve CVS yapısında raporlar alınabilmelidir
     65. Auto Discovery ile bilinmeyen log kaynakları tespit edilip otomatik olarak sisteme eklenebilmelidir.
     66. Ham (Raw) datalar için integrity kontrolü sağlanmalıdır. Ham veriler kurumun sağlayacağı harici disk alanında saklanacaktır.
     67. Log Manager üzerinde yapılacak raw data aramalarında strings (Örn:Confidential) ve integers(Örn:IP adres) ve regex kullanılabilmelidir.
     68. Log Manager için sıkıştırma oranı ayarı ile hem performans hem de kapasite planlaması yapılabilmelidir.
     69. Log Manager, lokal hdd, SAN, CIFS, NFS yoluyla storage pool yaratabilmelidir. Bu poollar log kaynakları temelinde özelleştirilebilmelidir.
     70. Log Manager üzerinden tarihsel ve arşivlenmiş veri üzerinde tarama yapmak mümkün olmalıdır.
     71. Merkezi yönetim arabirimi üzerinden delil araştırmaları yapılırken; farklı kaynaklardan kategorize edilmiş parametreler “ve, veya, değil” gibi mantıksal işlemlerle birleştirilebilecektir.
     72. Oluşan tehdit görünümlerinde Bugtrak, ICE, CVE gibi referans bilgileri gösterilebilmelidir
     73. Yaratılan kurallara istinaden oluşan olaylarla ilgili alarmlar oluşturulabilmelidir. Oluşan alarmlar; ilgili kişilere atanabilmeli, kayıtlanabilmeli, case açılabilmeli, görsel uyarı oluşturulabilmeli, sms ve e-mail atabilmeli, ozel bir script çalıştırılabilmelidir.
     74. Network cihazlarından gönderilen SNMP trapleri ve flow dataları sistem tarafından toplanabilmelidir.
     75. Çözüm ip temelli Ağ tarama özelliğine sahip olmalı bu yolla ağ içerisindeki varlıkların tespiti mümkün olmalıdır. Tespit edilen varlıklar otomatik gruplandırılabilmelidir
     76. Toplanan logların kaynağı ne olursa olsun normalizasyon desteklenmelidir.
     77. Uzun dönem log kayıtlarının rapor ve disk alanı açısından optimizasyonu nedeniyle log aggregation teknikleri desteklenmelidir.(Belli süre içerisinde gerçekleşen, aynı tipteki benzer olaylara ait kayıtların tek bir kayıt şeklinde gösterilmesi)
     78. Ara yüz üzerinde EPS değeri, log istatistikleri ve alarmlar görülebilecektir.
     79. Çözüm Active Directory ve/veya Radius kimlik doğrulama yöntemlerini kullanabilmeli bu yollar kullanıcı tanımları ile eşleştirmek mümkün olmalıdır. Ayrıca raporlarda, olay görünümlerinde ve korelasyon kurallarında AD yoluyla filtreleme imkanı sağlanmalıdır.
     80. Kullanıcılar için farklı gruplar tanımlanabilmeli, grup için yetkili kılınan device’lar, politikalar ve zone lar atanabilmelidir. Böylece grup içerisindeki bir kullanıcı yetkileri dahilindeki cihazlar, politikalar ve zone’lara erişimi sağlanmalıdır. Kullanıcılar kendi ara yüzlerini kişiselleştirebilecektir.
     81. Geo Location, IP kaynak ve hedefleri, Port, Application, Host gibi kriterleri istinaden izleme listeleri tanımlanabilmeli bu tanımlar alarm kuralları kapsamında kullanılabilmelidir. Dolayısıyla örneğin sadece bir IP bloğu ile ilgili oluşan olaylar belli eşik değerlerde olay oluşturması durumunda görsel ve işitsel uyarılar oluşturabilmeli ve özel rapor ya da görünüm ekranlarında izlenebilir yapıda olmalıdır. Görsel ekranlar grafiksel kalıpların dışında network topoloji ve Geo Location haritalar şeklinde sağlanmalıdır
     82. Alarm oluşturulurken birden fazla kriter seçilebilmeli ve oluşturulacak alarmlar için ticket oluşturulabilmeli ve ticketin’in atandığı kullanıcılara tarafından aksiyon alınmaması durumuna belirlenen zaman sonrasında farklı bir kişiye risk seviyesi yükseltilerek atanabilmeli.
     83. Teklif edilecek sistem API ile erişime destek vermelidir.
     84. Teklif edilecek çözüm toplanan logu başka veri kaynakları ile zenginleştime kabiliyeti sağlamalıdır.
     85. En az 450 farklı log tipi için hazır log tanıma bileşeni bulunmalıdır. Otomatik ya da manuel güncellemelerle bu veri tabanı gelişen yapıda olmalıdır.
     86. Loglar en az 1:20 oranında sıkıştırılabilmelidir. Bu sıkıştırma oranları GUI üzerinden ayarlanabilir yapıda olmalıdır.
     87. Çözüm 1 yılı içerecek şekilde lisanslanmalı lisans suresi boyunca üreticinin destek merkezine sorun bildirilebilmelidir.
  2. **VERİ TABANI GÜVENLİĞİ ÇÖZÜMÜ**
     1. Önerilecek veritabanı güvenlik çözümü; SQL sunucular için DB aktivite ve takibi, sanal yama güvenliği ve zaafiyet tespitinden oluşacaktır. Çözüm engelleme kabiliyeti sağlayabilmelidir.
     2. DB aktivite ve takip çözümü ajan temelli olup en az aşağıdaki işletim sistemleri ve veri tabanı çözümlerini desteklemelidir:
     3. Microsoft Windows 20012 veya üzeri (32bit, 64 bit ve Itanium), Red Hat Linux 7.0 ve sonrası, SUSE Linux 11.4, 12.2 ve sonrası ya da CentOS 7 ve sonrası sürümleri, Oracle Linux 6 ve sonrası
     4. Oracle 8i ve üzeri - Oracle RAC ve Oracle Exadata dahil (Solaris, IBM AIX, Linux, HP-UX, MS Windows)
     5. Microsoft SQL Server 2000 ve üzeri
     6. PostgreSQL 9.3 ve üzeri
     7. SAP HANA SPS 09, R91 ve sonrası
     8. Sybase ASE 12.5 ve sonrası
     9. MariaDB 5.5 (5.5.32 ve sonrası), 10.0 ve 10.1 (Linux)
     10. MySQL 5.1 ve sonrası (4.6, 4.7, 5.2 ve 5.3)
     11. Teradata 12, 13, 13.10, 14.15, ve 15.1 (Linux)
     12. IBM DB2 9.5 ve sonrası (Linux, Unix ve windows)
     13. Çözüm SQL aktivitelerini takip edebilmek için ağ üzerinden her hangi bir yönlendirmeye (SPAN, Mirror, TAP, Proxy) ihtiyaç duymamalı ve ağ yapısında bir değişikliğe sebep olmamalıdır.
     14. Çözüm FIPS uyumluluğu sağlayabilmelidir.
     15. Çözüm PCI-DSS, Sabanes Oxley (SOX), SAS-70, GLBA, HIPAA regülasyonları ve en iyi yapılandırma (Best Practise) için ücretsiz olarak hazır şablonlar sunmalı.
     16. Zaafiyet tespit ağ temelli olmalı ve herhangi bir ajan gerektirmemelidir. Zaafiyet tespit modulu en az 6000 adet zaafiyete sahip olmalı ve guncelleme mantığıyla genişlemeye imkan sağlamalıdır.
     17. Sanal yama (Virtual Patch) özelliği ile SQL sunucular üzerinde bulunan yama açıklarına ve ataklara karşı koruma sağlamalıdır. En az 600 adet ön tanımlı kural sunmalıdır.
     18. Entegre veri tabanı güvenliği çözümünün merkezi yönetim modulu, aynı üreticinin son kullanıcı antivirus, encyption, HostDLP, Host IPS, application control, change control ürünlerinide aynı zamanda yönetebilen ara birim olmalı, bu arabirim Microsoft Windows 2008 R2, 2012, 2012 R2 veya 2016 üzerinde çalışabilmelidir. Backend veritabanı olarak ise Microsoft SQL server 2008, 2008 R2, 2012, 2014 veya 2016 kullanabilmelidir.
     19. Entegre veri tabanı güvenliği çözümünün merkezi yönetim modülü istenmesi durumunda standalone olarak çalışabilmeli ve aşağıda belirtilen İşletim sistemlerini desteklemelidir:
     20. Microsoft Windows 2008, 2008 R2, 202, 2012 R2 ve 2016
     21. Linux RedHat 4.0 ve sonrası, SUSE Linux 10.0 ve sonrası, CentOS 4 ve sonrası,
     22. Entegre veri tabanı güvenliği çözümünün merkezi yönetim modülünün Standalone sürümü backend veri tabanı olarak MS SQL 2008, 2008 R2, 2012, 2014 sürümleri ve Oracle 11g ve sonrasında çalışabilmelidir.
     23. Entegre veri tabanı güvenliği çözümünün merkezi yönetim modülü istenmesi durumunda ücretsiz olarak Cluster yapısında çalışabilmeli.
     24. Teklif edilecek yazılımlar, veri tabanı konusundaki genel güvenlik problemlerini çözebilecek ve kurum içinden gelebilecek tehditleri tespit edebilecek özelliklere sahip olmalıdır.
     25. Çözüm ağ üzerinde çalışan veri tabanlarını tespit edebilmelidir.
     26. Teklif edilen çözüm, yetkisiz ip lerden gelen kullanıcıların veritabanına erişimini tespit edebilmeli ve engelleme kabiliyeti gösterebilmelidir.
     27. Teklif edilen çözüm, yönetim yazılımına yetkisiz kullanıcıların login olmasını engellemelidir.
     28. Teklif edilen çözüm kullanılarak veri tabanında çalıştırılabilecek her türlü komutun kullanımı tespit edilebilmeli veya kurallara bağlanabilmelidir.
     29. Çözüm üzerinde her hangi bir kural oluşturulmadan yada aktif edilmeden takip edilen veri tabanı sunucularına bağlanan uygulama, ip ve kullanıcı bilgileri için baseline oluşturulmalı ve sunulmalıdır.
     30. Entegre veri tabanı güvenliği çözümü regülasyonlara uyumluluk açısından kullanıcılar, uygulamalar tarafından çalıştırılan sorguların sonuçlarını (cevaplarını) saklamamalı, sadece sorgunun kendisini tutmalıdır.
     31. Kullanıcılar tarafından çalıştırılan belirli kritik sorgular için maskeleme yapabilmelidir. Bu şekilde sorgu içerisinde yer alan kritik bir bilgi veri tabanı güvenlik yazılımının yöneticisi tarafından görülemeyecektir.
     32. Kullanıcılar tarafından çalıştırılan sorguların SQL sunucu üzerinde hata oluşturması durumunda bu olayları tespit edebilecek bir yöntem sunmalıdır
     33. Kullanıcılar tarafından çalıştırılan uzun sorguların tespit edilebilmesini sağlayacak bir yöntem sunmalıdır.
     34. SQL sunucular üzerinde standart olmayan portlar üzerinden yapılan aktiviteler trafiğin şifreli olması (IPSec, SSL ve benzeri) fark etmeksizin tespit edilebilmelidir
     35. Güvenlik ile ilgili olarak yapılmış olan tanımlamaların kullanımı veya bu tanımlamaları aşma girişimleri denetlenebilmeli ve raporlanabilmelidir
     36. Uç kullanıcılar tarafından gerçekleştirilen işlemler tetikleyici (trigger), saklı prosedür (stored procedure) ve fonksiyonlar (function) içerisinde de yapılsa tespit edilerek engellenebilmelidir.
     37. Uç kullanıcı ile veri tabanı sunucusu arasındaki trafiğin şifrelenmesi durumunda da tanımlı güvenlik kuralları çalışabilmelidir.
     38. SQL sorgu seviyesinde audit yapabilecektir. (SELECT SQL statements)
     39. Önerilen çözümün veritabanı ajanı shared memory de çalışmalı ve tüm query ve DB erişimleri(tablolar dahil) izlenebilmelidir.
     40. Insert,update,delete gibi komut aktiviteleri izlenebilmelidir.
     41. Ajan ile yönetim sunucusu arasında ki bağlantının kesilmesi durumunda mevcut politikalar uygulanmaya devam etmeli ve yönetim sunusu ile aradaki bağlantı tekrar sağlandığında olaylar gönderilmelidir.
     42. Ajan ile yönetim sunucusu arasındaki bağlantı şifreli olarak gerçekleştirilmelidir.
     43. SQL aktivitelerinin takibi için kullanılan kurallarda yapılan değişiklikleri saklamalı ve kurallar arasında karşılaştırma yapılabilmesine imkan sağlamalıdır.
     44. Çözüm hazır rapor şablonları ile gelmeli ve raporlar html, ve PDF olarak üretilebilmelidir.Raporlar otomatik olarak e-posta ile ilgilileri ulaştırılabilmelidir.
     45. Raporlar içerisinde veri tabanı sunucusu, IP adresleri, seviye, OS kullanıcısı, kullanıcı, kural ve ajan parametrelerine göre guruplama imkanı sağlamalı. 2 farklı guruba göre (IP ve Kullanıcı) raporlar süzülebilmelidir.
     46. Önerilen çözüm hazır audit şablonları ile sunulmalıdır.
     47. Kural yazma ekranı akıllı sihirbaza sahip olmalı olası syntax sorunları uyarılmalı ve cumle yazımına yardımcı olmalıdır.
     48. Kural ihlalleri durumunda proaktif uyarı mekanizmaları olmalı, bu uyarılar syslog, email ile gönderilebilmelidir..
     49. Zaafiyet tespit modulü, veri tabanı sunucularının patch durumunu, zayıf şifrelere sahip olup olmadığını tespit edebilmelidir. Backdoor tespiti yapabilmeli,PL/SQL kodlarında herhangi bir güvenlik sorunu olup olmadığını raporlayabilmelidir. Elile yazılmıs ozel kontrol kurallarına imkan sağlamalıdır(Custom check)
     50. Veri tabanı güvenlik çözümü session’ın terminate edilmesi dışında kullanıcıyı belli süre ile karantinaya alabilmelidir.
     51. Veri tabanı platformunun VM olması durumunda sanal sistemleri arasındaki veri iletisiminin denetlenmesi mumkun olmalıdır.
     52. Hassas verilerin veri tabanı tablolarında olup olmadıgının tespiti mumkun olmalıdır(PII,SSN vb..).Ayrıca ağ üzerinde hazlihazırda çalışan veri tabanlarının keşfi mümkün olmalıdır.
     53. Rootkit vb. şüpheli davranışların neden olduğu değişiklikler tespit edilebilmelidir.
     54. Tespit edilen zaafiyet tespitlerine istinaden detaylı duzeltme raporları sunulabilmelidir.
     55. Merkezi Yönetim arayüzü üzerinden veri tabanı guvenliği çözümü için farklı rollerde adminler atanabilmelidir. Kullanıcı tanımlamalarında LDAP,MS AD yoluyla mevcut kullanıcı veritabanından faydalanılabilmelidir.
     56. Denial of service,SQL injection,buffer overflow vb saldırı tipleri denetlenip engellenebilmelidir.
     57. Önerilen çözüme ait ajanın veri tabanı sunucusuna kurulması sonrası, güncellenmesi, upgrade edilmesi, kaldırılması gibi işlemlerde herhangi bir reboot ve servisin yeniden başlatılma gereksinimi olmamalıdır.
     58. Ajanların bir sebepten dolayı stop edilmesi durumunda yönetim sunucusu üzerinden bu durum görülmeli ve alert edilebilmelidir.
     59. Ajanların durdurulmaya karşı korunması için aynı üreticiye ait uç nokta güvenlik yazılımı ile entegre olarak koruma sağlayabilmelidir.
     60. Güncelleme işlemleri isteğe bağlı olarak sadece uyarı, yeni sürüm yayınlandığı anda anlık olarak yüklenme veya belirli günlerde ve saatlerde otomatik olarak yüklenebilmelidir.
     61. Yönetim yazılımı üzerinde SQL aktivitelerine ait eski olayların arşivlenmesini ve şifreli bir şekilde tutulmasını sağlamalıdır.
     62. Arşivlenen olaylar çözümün veri tabanına restore edilmeden mount edilme yöntemi ile yüklenebilmeli ve işlemler sonrasında yükleme işlemi iptal edilebilmelidir. Bu şekilde eski arşivlenmiş olaylara hızlı bir şekilde erişim sağlanmalıdır.
     63. Çözüm tarafından tespit edilen olaylar için terminate session, arşivleme, SNMP Trap, Syslog, Windows Event Log, disk üzerinde belirli bir alana alert yazabilme ve email gönderebilme askiyonları sağlanabilmelidir.
     64. Çözüm tarafından tespit edilen olaylar SIEM çözümlerine syslog üzerinden CEF formatında gönderilebilmelidir.
     65. Teklif edilecek çözüm 1 instance sayısına gore 1 yıl olacak şekilde lisanslanacaktır. Lisans süresi boyunca son kullanıcı üreticinin support ekibine 7x24 e-mail veya telefon ile sorun bildirebilecektir.
  3. **UÇ NOKTA GÜVENLİĞİ ÇÖZÜMÜ**

**Uç Nokta Güvenliği Çözümü Genel Özellikleri :**

* + 1. Teklif edilen sistem, merkezi yönetim sistemi ve istemci ajanı bileşenlerinden oluşmalıdır.
    2. Çözümün uç nokta bileşenleri aynı üretici tarafından geliştirilmiş olmalı ve tek bir kurulum dosyası ile yükleme sağlanabilmelidir.
    3. Teklif edilecek çözüm, aynı üreticiye ait EDR fonksiyonuna sahip olmalı, ek bir lisans alımı ile EDR fonksiyonu ek bir ajan kurulumu gerekmeksizin mevcut ajan üzerinde etkinleştirilebilmelidir.
    4. Teklif edilecek çözüm, ek bir lisans alımı ile sağlanabilen EDR fonksiyonu ile, aynı üreticiye sahip gelişmiş/hedef odaklı saldırılardan koruma platformu ve bu platformun sahip olduğu sandbox çözümü ile entegre olabilmelidir.
    5. Teklif edilecek çözüm, aynı üreticinin sahip olduğu uygulama ve web siteleri repütasyon verilerini ve yeni tehdit bilgilerini sağlayan global bir tehdit istihbaratı veritabanı ile entegre çalışabilmelidir.

**Uç Nokta Koruma Bileşeni Özellikleri :**

* + 1. Teklif edilecek antivirüs yazılımı aşağıda belirtilen işletim sistemleri üzerinde çalışabilmelidir.
    2. Microsoft Windows:
    3. Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 veya üstü;
    4. Windows 8 Professional / Enterprise;
    5. Windows 8.1 Professional / Enterprise;
    6. Windows 10 Home / Pro / Education / Enterprise.
    7. Windows Small Business Server 2011 Essentials / Standard (64 bit)
    8. Windows MultiPoint Server 2011 (64 bit);
    9. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 veya üstü;
    10. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
    11. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
    12. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
    13. Microsoft Windows Server 2019 Essentials / Standard / Datacenter.
    14. Linux:
    15. Pardus OS Türkçe v19.1
    16. Ubuntu 16.04 LTS and later
    17. Ubuntu 18.04 LTS and later
    18. Red Hat Enterprise Linux 6.7 and later
    19. Red Hat Enterprise Linux 7.2 and later
    20. Red Hat Enterprise Linux 8.0 and later
    21. CentOS 6.7 and later
    22. CentOS 7.2 and later
    23. CentOS 8.0 and later
    24. Debian GNU / Linux 9.4 and later
    25. Debian GNU / Linux 10.1 and later
    26. Oracle Linux 7.3 and later
    27. Oracle Linux 8 and later
    28. SUSE Linux Enterprise Server 12 SP3 and later
    29. SUSE Linux Enterprise Server 15 and later
    30. openSUSE Leap 15 and later
    31. ALT 8 SP Workstation
    32. ALT 8 SP Server
    33. ALT Workstation 8
    34. ALT Workstation K 8
    35. ALT Server 8
    36. ALT Education
    37. ALT Workstation 9
    38. ALT Server 9
    39. ALT Education 9
    40. Amazon Linux AMI
    41. Linux Mint 18.2 and later
    42. Linux Mint 19 and later
    43. Astra Linux Special Edition, version 1.5 (generic and PaX kernel)
    44. Astra Linux Special Edition, version 1.6 (generic and PaX kernel)
    45. Astra Linux Common Edition, version 2.12
    46. OS ROSA Cobalt 7.3 for client systems
    47. OS ROSA Cobalt 7.3 for server systems
    48. GosLinux 6.6
    49. GosLinux 7.2
    50. AlterOS 7.5 and later
    51. MacOS :
    52. macOS 10.15
    53. macOS 10.14
    54. macOS 10.13
    55. macOS 11
    56. Mobil :
    57. Android 4.2-11.0
    58. iOS 10.0 – 14.0
    59. iPadOS

**Microsoft Windows işletim sistemleri için:**

* + 1. Tercih edilecek çözüm ağdan gelebilecek olan saldırılara karşı koruma sağlamalıdır.
    2. Teklif edilecek çözümün uç noktalar için aygıt kontrolü fonksiyonu bulunmalıdır.
    3. Teklif edilecek çözüme ait aygıt kontrolü özelliği ile, depolama aygıtları ve diğer çevre birimleri (yazıcı, floppy disk, CD/DVD sürücüsü, modem, akıllı kart, taşınabilir cihaz, bluetooth) üzerinde erişim hakları kullanıcı bazlı olarak kontrol edilebilmeli ve bu haklar kullanıcı bazlı olarak tanımlanabilmelidir.
    4. Teklif edilecek çözüm ile uç noktalarda hard disk, floppy disk, çıkarabilir disk ve ağ sürücüleri üzerinde virüs ve zararlı yazılım taraması yapılabilmelidir.
    5. Teklif edilecek çözüm, bellekte bulunan virüslerin/zararlı yazılımları tespit edebilmeli ve engelleyebilmelidir.
    6. Teklif edilecek çözüm, uç noktalarda bilerek/bilmeyerek veya zararlı yazılımlar aracılığı ile fonksiyonlarını durdurmaya yönelik müdahalelere karşı kendini koruma yeteneğine sahip olmalıdır.
    7. Teklif edilecek çözüm, yazılımsal firewall bileşenine sahip olmalıdır.
    8. Teklif edilecek çözüm, uç noktalarda donanım envanter bilgisi çıkarabilmeli ve bu bilgileri yönetim modülüne aktarabilmelidir.
    9. Teklif edilecek çözümün, uç noktalarda yüklü yazılımların envanter bilgisini çıkarabilmelidir.
    10. Teklif edilecek çözüme ait uç nokta koruma bileşeni ile çıkarılan envanter bilgisi, uç nokta ajanı üzerinden veya merkezi yönetim bileşeni üzerinden en az PDF formatında dışa aktarılabilmelidir.
    11. Teklif edilecek çözüm, hijacking’e karşı sistem üzerinde bulunan programların herhangi bir programın altına çalışması halindeki süreci denetleyebilmelidir.
    12. Teklif edilecek çözüm, web kaynakları için erişim kontrolü özelliği bulunmalıdır. Web filtreleme politikaları , kategori ve indirilebilir içerik türüne göre erişim politikaları yürütülebilmelidir.
    13. Teklif edilecek çözüm, e-posta istemcisine bağlı olmadan POP,IMAP,SMTP,MAPI,NNTP protokollerini ve e-posta trafiğini kötü amaçlı yazılımlara karşı kontrol edebilmelidir.
    14. Teklif edilecek çözüm, host bazlı çalışan saldırı önleme sistemi (HIPS) özelliği bulunmalıdır.
    15. Teklif edilecek çözüm, uygulama kontrolü modülüne sahip olmalıdır.
    16. Teklif edilecek çözüm, uygulama yükleme/başlatma kontrolü sayesinde uygulamaların belirlenen kurallar doğrultusunda çalışmasını ve yönetilebilmesini sağlayabilmelidir.
    17. Teklif edilecek çözüm, uygulama yetki kontrolü özelliğine sahip olmalı ve korumalı makinelerde programların yüklenmesini ya da çalıştırılmasını engelleyebilmelidir. Bu bileşen ile klasör adresini, metadata bilgisini ve MD5 kontrolünü ayrıca izleyebilir nitelikte olmalıdır.
    18. Teklif edilen çözümün, uç nokta ajanı aracılığı ile korunan bilgisayarlarda uzaktan tarama ve uzaktan komut çalıştırma fonksiyonları olmalıdır.
    19. Teklif edilecek çözüm ile, korunan makineler gruplandırılabilmeli her bir gruba farklı politikalar uygulanabilmelidir.
    20. Teklif edilecek çözüm, dosya, klasör, dahili disk ve bunun yanında çıkarılabilir disk bazında 256 bit AES şifreleme sağlayabilmelidir.
    21. Teklif edilecek çözüm, sezgisel analiz yeteneğine sahip olmalı, öncelikli kötü amaçlı yazılımları engellemeye ve tanımlamaya olanak sağlaması bunun ile birlikte uygulamaların davranışlarını analiz etmesi ve takibe alması gereklidir.
    22. Teklif edilecek çözüm ile, manuel ve otomatik olarak uygulamalar ve işletim sistemleri için zafiyet ve yama tespiti yapılabilmeli ve eksik yamalar merkezi yönetim bileşeni üzerinden yüklenebilmelidir.
    23. Teklif edilecek çözüm, uç nokta ajanı üzerinde kullanıcıya konfigürasyona müdahale yetkisi vermeye veya müdahaleye izin vermeyecek şekilde yetkilendirmelere izin vermelidir.
    24. Teklif edilecek çözüm, uç nokta ajanı üzerinde, ajanın alacağı her bir aksiyon için kullanıcıya gösterilecek uyarı mesajlarıyla ilgili ayrı ayrı bilgilendirme ayarları yapılabilmesine izin vermelidir.
    25. Teklif edilecek çözüm, uç nokta ajanı üzerinde, merkezi yönetim bileşeni üzerinde tanımlanmış belirli görevlerin düzenli olarak veya manuel olarak çalıştırılmasına izin vermelidir.

**Linux işletim sistemleri için:**

* + 1. Teklif edilecek çözüm Linux işletim sistemleri için yerleşik antivirüs motoru ile zararlı yazılımlara karşı koruma sağlamalıdır.
    2. Teklif edilecek çözüm ile uç noktalarda hard disk ve ağ sürücüleri üzerinde virüs ve zararlı yazılım taraması yapılabilmelidir.
    3. Teklif edilecek çözüm, tarama dışı bırakılacak dosya ve dosya yolları tanımlamaya imkan sağlamalıdır.
    4. Teklif edilecek çözüme ait politikalar aktif, ofis dışı ve inaktif olarak ayarlanabilmeli, istemci makinelere kurum ağında ve kurum ağı dışında farklı politikalar uygulanabilmelidir.
    5. Teklif edilecek çözüm, , oluşturulacak grupların her biri için farklı politikalar uygulamayı ve tüm gruplarda geçerli olabilecek şekilde politika devralma fonksiyonunu desteklemelidir.
    6. Teklif edilecek çözüm zamanlanmış antimalware taramalarına izin vermeli ve zamanlanmış taramalar için aşağıdaki seçenekleri desteklemelidir:
    7. Her N saatte bir
    8. Her N günde bir
    9. Her N dakikada bir
    10. Haftanın belirtilen gününde
    11. Ayın belirtilen gününde
    12. Belirtilen zaman için 1 defa
    13. Uygulama güncellemesinden sonra
    14. Uygulama her başlatıldığında
    15. Virüs salgını tespit edildiğinde
    16. Belirtilen görev başarıyla tamamlandığında
    17. Belirtilen görev başarısız olduğunda
    18. Teklif edilecek çözüm ile sıkıştırılmış dosyaların taranması mümkün olmalıdır.
    19. Teklif edilecek çözüm, Linux işletim sistemi üzerinde zararlı olarak tespit edilmiş dosyalar için karantina desteğine sahip olmalıdır.
    20. Teklif edilecek çözüm, belirtilen özelliklere ek olarak uç nokta ajanında aşağıdaki bileşenlere sahip olmalıdır:
    21. Güvenlik Duvarı (Firewall)
    22. Dosyalar için Tehdit Koruması (File Threat Protection)
    23. Anti-Cryptor (Ransomvare vb. şifreleme zararlı yazılımlarına karşı)
    24. Aygıt Denetimi (Device Control)
    25. Web Tehdit Koruması (Web Threat Protection)
    26. Ağ Tehdit Koruması (Network Threat Protection)
    27. Dosya Bütünlüğü İzleme (File Integrity Monitoring)
    28. Sezgisel (heuristic) analiz
    29. Davranışsal (behavior) analiz
    30. Teklif edilecek çözüm, uç nokta ajanı üzerinde kullanıcıya konfigürasyona müdahale yetkisi vermeye ve ayrıca müdahaleye izin vermeyecek şekilde yetkilendirmelere izin vermelidir.
    31. Teklif edilecek çözüm, uç nokta ajanı üzerinde, merkezi yönetim bileşeni üzerinde tanımlanmış belirli görevlerin düzenli olarak veya manuel olarak çalıştırılmasına izin vermelidir.
    32. Teklif edilecek çözüm, konfigürasyonlarda yapılan değişikliklerle birlikte, eski konfigürasyon dosyalarını kayıt altına alabilmeli ve kayıtlı konfigürasyon dosyalarında değişiklikleri karşılaştırabilmelidir.

**Android ve IOS mobil işletim sistemleri için:**

* + 1. Teklif edilen çözüm ile, kişisel bilgisayar ile senkronizasyon ve bir tarayıcı üzerinden dosya indirme işlemi sırasında kablosuz bağlantılar (infrared bağlantı noktası, Bluetooth), EMS ve MMS kablosuz bağlantıları yoluyla aktarılan tüm gelen nesneler taranabilmelidir.
    2. Teklif edilen çözüm ile, kullanıcının isteği üzerine veya zamanlanmış olarakmobil cihaz veya bağlı bellek genişletme kartı üzerindeki dosya sistem nesneleri taranabilmelidir.
    3. Teklif edilen çözüm ile, istenmeyen SMS ve MMS ler engellenebilmelidir.
    4. Teklif edilen çözüm ile, hırsızlığa karşı koruma işlevi ile mobil cihaz bloke edilebilmeli, verilerin ve kişi kayıtları silinebilmeli, kayıp cihazın yeri GPS olanakları ile tespit edilebilmelidir.

**Uç Nokta Güvenliği Çözümü - Merkezi Yönetim Bileşeni Özellikleri :**

* + 1. Teklif edilecek olan yönetim modülü aşağıda belirtilen işletim sistemleri üzerinde çalışabilmelidir.
    2. Microsoft Windows 10 20H2 32-bit/64-bit (only for version 12.2 and later)
    3. Microsoft Windows 10 20H1 32-bit/64-bit (only for version 12.1 and later)
    4. Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
    5. Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit
    6. Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit
    7. Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit
    8. Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit
    9. Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit
    10. Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit
    11. Microsoft Windows 10 Pro 19H1 32-bit/64-bit
    12. Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
    13. Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
    14. Microsoft Windows 10 Education 19H1 32-bit/64-bit
    15. Microsoft Windows 10 Pro 19H2 32-bit/64-bit
    16. Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
    17. Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
    18. Microsoft Windows 10 Education 19H2 32-bit/64-bit
    19. Microsoft Windows 8.1 Pro 32-bit/64-bit
    20. Microsoft Windows 8.1 Enterprise 32-bit/64-bit
    21. Microsoft Windows 8 Pro 32-bit/64-bit
    22. Microsoft Windows 8 Enterprise 32-bit/64-bit
    23. Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
    24. Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
    25. Windows Server 2019 Standard 64-bit
    26. Windows Server 2019 Core 64-bit
    27. Windows Server 2019 Datacenter 64-bit
    28. Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
    29. Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
    30. Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
    31. Windows Server 2016 Standard (LTSB) 64-bit
    32. Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
    33. Windows Server 2016 Datacenter (LTSB) 64-bit
    34. Windows Server 2012 R2 Standard 64-bit
    35. Windows Server 2012 R2 Server Core 64-bit
    36. Windows Server 2012 R2 Foundation 64-bit
    37. Windows Server 2012 R2 Essentials 64-bit
    38. Windows Server 2012 R2 Datacenter 64-bit
    39. Windows Server 2012 Standard 64-bit
    40. Windows Server 2012 Server Core 64-bit
    41. Windows Server 2012 Foundation 64-bit
    42. Windows Server 2012 Essentials 64-bit
    43. Windows Server 2012 Datacenter 64-bit
    44. Windows Storage Server 2016 64-bit
    45. Windows Storage Server 2012 R2 64-bit
    46. Windows Storage Server 2012 64-bit
    47. Teklif edilecek olan yönetim modülü aşağıda belirtilen veritabanları üzerinde çalışabilmelidir.
    48. Microsoft SQL Server 2012 Express 64-bit
    49. Microsoft SQL Server 2014 Express 64-bit
    50. Microsoft SQL Server 2016 Express 64-bit
    51. Microsoft SQL Server 2017 Express 64-bit
    52. Microsoft SQL Server 2019 Express 64-bit
    53. Microsoft SQL Server 2014 (tüm sürümler) 64-bit
    54. Microsoft SQL Server 2016 (tüm sürümler) 64-bit
    55. Microsoft SQL Server 2017 (tüm sürümler) on Windows 64-bit
    56. Microsoft SQL Server 2017 (tüm sürümler) on Linux 64-bit
    57. Microsoft SQL Server 2019 (tüm sürümler) on Windows 64-bit
    58. Microsoft SQL Server 2019 (tüm sürümler) on Linux 64-bit
    59. MySQL Standard Edition 5.7 32-bit/64-bit
    60. MySQL Enterprise Edition 5.7 32-bit/64-bit
    61. All supported SQL Server editions in Amazon RDS and Microsoft Azure cloud platforms
    62. MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine
    63. Teklif edilecek çözüme ait merkezi yönetim sistemi, Windows Failover Clustering desteği sağlamalıdır.
    64. Tercih edilecek çözüm, merkezi yönetim sistemi üzerinden uç noktalara koruma paketlerine ait güncellemeleri ve yazılımsal güncellemeleri dağıtabilmeli ve bu dağıtımlar zamanlanmış olarak ayarlanabilmelidir.
    65. Teklif edilen çözüm ile, uç nokta ajanı dağıtılmış tüm uç nokta/kullanıcı makineleri, sunucular ve mobil cihazlar merkezi ve birleşik bir yönetim sistemi tarafından yönetilebilmelidir.
    66. Teklif edilecek çözüm ile, sistemde varolan koruma bileşenlerine ait davranışlar ve bu davranışlara ait kayıtlar merkezi yönetim sistemi üzerinden izlenebiliyor ve kayıt altına alınabiliyor olmalıdır.
    67. Teklif edilen çözüm, yönetim konsolu üzerinde son güncellemeleri geri alma özelliğine sahip olmalıdır ve bu fonksiyon ile güncelleme sonrasında yaşanabilecek bir sorun anında geriye dönülebilmelidir.
    68. Teklif edilecek çözüme ait yönetim modülü, üçüncü parti araçları kullanmadan Active Directory ile entegre olarak veya domain ortamında olmayan makineler için bu makinelerde geçerli ve yetkili bir kullanıcı hesabıyla uzak kurulum opsiyonu ile koruma bileşenlerinin dağıtımını yapabilmelidir.
    69. Teklif edilecek çözüme ait yönetim konsolu üzerinde manuel kurulum paketleri oluşturulabilmelidir.
    70. Teklif edilecek çözüme ait yönetim modülü, hedef bilgisayarlarda üretici tarafından tanımlanabilen ve bu makinelerde çalışmakta olan uygulamaların güvenlik açıklıklarını raporlayabilmelidir.
    71. Teklif edilen çözüm, uç nokta ajanı ile tespit edilen güvenlik açıklıklarını kapsayacak güncellemelerin, uzaktan korunan bilgisayara dağıtım işlemini yapabilmelidir.
    72. Teklif edilecek çözüme ait yönetim modülü üzerinde, takibi yapılan tüm kullanıcı, sistem hareketlerinin yanında zararlı yazılım tespit raporlarının da bilgisi grafiksel bazda gösterilmelidir.
    73. Teklif edilen çözüm, yönetim modülü üzerinde konfigürason yedeği alabilmelidir.
    74. Teklif edilen çözüm ile, silinen dosyaların kopyalarını/yedeklerini merkezi yönetim modülü üzerinde depolayabilmelidir.
    75. Teklif edilen çözüme, sistem üzerinde PDF,EXCEL,HTM olarak tüm raporlar kayıt altına alabilmeli ve raporlar aynı formatta dışa aktarılabilmelidir.
    76. Çözüm, 1 yıl güncellemelerini alarak aktif faaliyette olacak şekilde şartnamede belirtilen tüm özellikleri sağlayacak bileşenleri ve lisansları ile 150 adet kullanıcı için teklif edilecektir.

1. **NETWORK TEKNİK ŞARTNAMESİ**
   1. **NETWORK AĞ ERİŞİM KONTROL SİSTEMİ**
      1. Teklif edilecek sistem en az aynı anda 7500 MAC adres destekleyecek lisans ile teklif edilecektir. Şartnamede istenilen tüm özellikler belirtilen sayıdaki mac adresinde destekleyecektir.
      2. Ağ erişim kontrol sistemi yazılım çözümü verilecektir. Yazılım çözümü ile VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V sanallaştırma platformu desteklenecektir.
      3. Ağ erişim kontrol sistemi merkezi mimaride çalışabilecek, gerekli kontrol ve erişim yetkilendirmelerini yapabilecektir.
      4. Teklif edilecek sistem; yönetim, raporlama, politika ve kural tanımlama fonksiyonlarını sağlayacaktır.
      5. Teklif edilecek sistem gelişmiş ve özelleştirilebilir raporlama sunacaktır. Kimlik doğrulama eğilimleri, daha önceden profil tanımlaması yapılmış cihazlar, kurum bünyesinde yer alan sabit ağ cihazları ve istenildiği takdirde kullanıcı bilgisayarlarının sağlık ve kurumun belirlemiş olduğu standartlara uygun olup olmadığına ilişkin veriler kullanımı kolay bir ekranda görüntülenebilecektir. Ayrıca kimlik doğrulama hatalarını izleme ve tespit için izleme listesi olacaktır.
      6. Ağ erişim kontrol sistemi kablolu, kablosuz ve VPN ağları için rol tabanlı ağ erişimini sağlayacaktır.
      7. Ağ erişim kontrol sistemi bağlanan kullanıcı ve bağlanılan cihaz özelliklerine bağlı olarak rol bazlı erişim yetkilendirme yapabilecektir.
      8. Teklif edilecek sistem son kullanıcı cihazlarına göre profil atayabilecektir.
      9. Ağ erişim kontrol sistemi son kullanıcı cihazlarına, cihaz tipine ve marka modeline göre farklı profil veya rol atayabilecektir.
      10. Ağ Erişim kontrol sistemi misafir ve çalışan yetkilendirmesi için misafir karşılama (captive portal) destekleyecektir. Bu captive portal ile misafirler bir sponsor izni ile sisteme dahil olabilirlerken kendi cihazlarını ofis ağına bağlamak isteyen şirket çalışanları ise Radius, Ldap ve Active Directory yetkilendirmesi ile sisteme kendi cihazlarını kaydedebilecektir.
      11. Ağ erişim kontrol sisteminin kurumdaki kablolu- kablosuz ağa dahil olacak misafirleri yönetmek ve ağa dahil etmek için misafir yönetimi çözümü desteği olacaktır. Misafir kullanıcıları özelleştirilebilir ara yüzler ile kendi kendilerini geçici şifreler ile ağa dahil edebilecektir.
      12. İstenilmesi durumunda misafirler ağa dahil olurken, ziyarete geldikleri kişilerin onayı gerekecek, istenirse bu onay ardından misafir kullanıcının şifresi cep telefonuna iletilecektir. İstenirse şifreler mail yoluyla da iletilebilecektir.
      13. Etkinliklerde etkinlik düzenleyenler toplu kullanıcı hesapları açabilecek ve bu hesaplar sadece etkinlik süresinde aktif olacaktır.
      14. LDAP/Active Directory ile uyumlu çalışabilecek, standartlara uygun kimlik depoları ile sorunsuz çalışabilecektir.
      15. Kullanıcılarla ilgili raporlar elde edilebilecektir.
      16. Akıllı cihazlar ile (akıllı telefon, tablet) uyumlu çalışabilecek, cihazlara özel arabirimler ile mobil cihazları destekleyecektir.
      17. Captive portal arayüzleri ile kullanıcılara bilgilendirme ekranları ya da reklam ekranları çıkarılabilecektir.
      18. Kullanıcının bağlandığı bölgeye göre bilgilendirme/reklam arayüzleri çıkarılabilecektir.
      19. FTP aracılığı ile yedekleme yapılabilecektir. Yedekleme gerçek zamanlı ya da önceden belirlenmiş bir zamanda; sistemin tamamı ya da bir kısmı için yapılabilecektir.
      20. 3. Parti sistemler için XML/RPC ya da SOAP API’ler sağlanacaktır.
      21. Web arabirimi, 802.1x ve 802.1x olmayan doğrulama ve yetkilendirmeleri destekleyecektir.
      22. Ayrıca IoT ve 802.1X desteği bulunmayan cihazlar için MAC adres doğrulamasını destekleyecektir. RADIUS tabanlı kimlik doğrulamanın uygulanamadığı kablolu ortamlar için, OnConnect ve SNMP tabanlı kimlik doğrulama yapabilecektir.
      23. RADIUS CoA desteği olacaktır.
      24. EAP-FAST, PEAP, TTLS, EAP-TLS, PAP, CHAP, MSCHAPv1 ve MSCHAPv2, EAP-MD5 desteği olacaktır.
      25. 3. Parti MDM (Mobil cihaz yönetimi) sistemleri ile uyumlu çalışabilecektir.
      26. İlgili çözüm hem kablolu kullanıcılar hem kablosuz kullanıcılar için kullanılabilecektir.
      27. Kablolu, kablosuz, VPN kullanıcıları için RADIUS sunucu özelliklerini destekleyecektir. Bu kullanıcılar için kimlik doğrulama, yetkilendirme ve accounting yapabilecektir.
      28. Teklif edilecek sistem 802.1x uyumlu ve CoA destekli ürünler için marka bağımsız tüm ağ cihazları ile uyumlu çalışabilecektir.
      29. RADIUS sistemi birden fazla Active Directory domaine dahil olabilecek ve bu kimlik depolarından kimlik doğrulaması ve yetkilendirme yapabilecektir.
      30. Kimlik doğrulamasını bir kimlik deposundan, yetkilendirmeyi başka bir kimlik deposundan yapabilecektir.
      31. İlave lisans ile teklif edilen sistem BYOD (Bring your own device) özelliği kullanılabilecektir. Teklif edilen kimlik doğrulama yazılımı ile birlikte kullanıcı cihazlarına sertifika ve VPN ayarlarını gönderbilecek ve istenildiğinde bu ayarları iptal edebilecek özellik için lisanslar istenildiğinde verilebilir durumda olacaktır.
      32. Teklif edilen sistem üzerinde Windows, MAC OSx istemcileri için NAC çözümü sağlanacaktır. İstenilmesi durumunda lisanslar ücretsiz olarak ilave edilebileceektir.
      33. Ağ Erişim kontrol sistemi ağ’a yeni katılan ve ağda bulunan cihazları aşağıdaki metotları kullanarak profilleyebilecektir. Bu Sayede IoT cihazlarıda otomatik olarak algılanabilecektir.
      34. DHCP isteklerini inceleyerek
      35. Http ve https isteklerine verilen cevapları inceleyerek
      36. IP aralığına göre
      37. Bulunduğu yere göre
      38. Ajan yüklü olup olmamasına göre
      39. SNMP isteklerine verdiği cevaplara göre
      40. SSH/Telnet isteklerine verdiği cevaplara göre
      41. TCP/UDP portlarının açık olup olmamasına göre
      42. Vendor OUI bilgisine göre
      43. Nmap tarama sonuçlarına göre
      44. İstenilmesi durumunda son kullanıcı kişisel bilgilsayarlarında ajan kurularak veya ajansız olarak aşağıda belirtilen tarama ve kontroller yapılabilecektir.
      45. Microsoft tabanlı işletim sisteminin tipi
      46. Microsoft tabanlı işletim sisteminin servis tipi
      47. Microsoft tabanlı işletim sisteminin güncelliği
      48. Antivirüs yazılımını yüklü olup olmadığı
      49. Antivirüs yazılımının güncelliği, marka bağımsız olarak versiyon kontrolü yapabilmeli, ilgili antivirüs yazılımının bir aydan daha eski olup olmadığını kontrol edebilmelidir.
      50. Bilgisayarda o anda çalışmakta olan servisler
      51. İstenilen uygulamanın o anda çalışıp çalışmadığı
      52. Bilgisayarın registry (kütük ) alanındaki bilgiler
      53. Bilgisayarın hardiskindeki dosyalar
      54. Ağ Erişim kontrol sistemi 3. parti sistemlere Syslog kullanarak gerçek zamanlı olarak bilgi paylaşma imkânı olacaktır. Bu sayede kullanıcılar ve cihazlar için ağda kimliği doğrulandıktan sonra değişen tehditlere anlık yanıt verebilmeli ve belirlenecek politikalara bağlı olarak anında güvenli ağ dışına alınabilecektir.
      55. Ağ erişim kontrol sisteminin IPv6 desteği olmalı ve IPv6 kimlik doğrulamayı destekleyecektir.
      56. Ağ erişim kontrol sistemi 3 yıl üretici destek paketi ile teklif edilecektir. Bu süre zarfında yazılım güncellemeleri ücretsiz yapılabilecektir.
      57. Teklif edilecek Ağ Kontrol Sistemi, mevcutta bulunan network alt yapısı ile birebir uyumlu olacaktır.
      58. Teklif edilen Ağ Kontrol Sistemi, mevcutta kullanılan ağ kontrol sistemi ile aynı üreticiye ait olmalıdır.
   2. **48 PORT POE KENAR ANAHTARLAR (37 ADET)**
      1. Anahtar üzerinde en az 12 adet mGig ve en az 36 adet 10/100/1000Mbps port bulunmalıdır. Herhangi bir fiber uplink portu kullanıldığında bu portlardan herhangi biri kullanım dışı kalmamalıdır.
      2. Anahtar 4 adet 1/10G fiber uplink porta sahip olmalıdır.
      3. Anahtarlama bant genişliği yığınlama kapasitesi hariç en az 392 Gbps olmalıdır. Anahtarın L2 anahtarlama performans değeri en az 291,66 Mpps olmalıdır.
      4. Anahtar en az 6MB paylaşımlı bir buffer’a sahip olmalıdır.
      5. Anahtarın bütün portlarında 802.3af (15W), 802.3at (30W) desteği olacaktır. Çift güç kaynağı ile 48 porttan aynı anda PoE+ (30W) sağlayabilecek donanıma sahip olmalıdır.
      6. Anahtar tekrar başlatıldığında dahi, kendine bağlı PoE cihazlarına kesintisiz güç vermeye devam edebilmelidir. Böylece anahtara bağlı PoE cihazlarının da reboot etmesi engellenmelidir.
      7. Anahtar IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.
      8. Anahtarın modüler güç kaynağı desteği olmalıdır. İkinci bir dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Yedek güç kaynağı anahtar çalışmaya devam ederken değiştirilebilmelidir. Anahtar yedek güç kaynağı ile teklif edilmelidir.
      9. Anahtar yedekli çalışan fan’lara sahip olmalıdır.
      10. Anahtar programlanabilir bir ASIC’e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.
      11. Anahtarın işletim sistemi modern programlama dillerinden NETCONF, RESTCONF ve YANG modellerini desteklemelidir.
      12. Anahtar en az 2GB DRAM ve 4GB Flash belleğe sahip olmalıdır.
      13. Anahtarın en az 9100 byte’lık jumbo frame desteği olmalıdır.
      14. Anahtarın bakır portlarında 802.3az EEE (Energy Efficient Ethernet) desteği olmalıdır.
      15. Anahtar envanter yönetimi için kullanılacak bir RFID etiketine sahip olmalıdır.
      16. Anahtar üzerinde veri merkezi içinde yerinin kolay bulunabilmesi için açılıp kapatılabilen mavi ışık (Blue Beacon) desteğine sahip olmalıdır.
      17. Anahtara opsiyonel olarak Bluetooth adaptör bağlanabilmeli, böylece bluetooth üzerinden anahtarın WEB ve komut arayüzüne erişmek, log ve işletim sistemi transferi yapmak mümkün olmalıdır.
      18. Yığınlama;Her anahtar üzerinde 2 adet yığınlama portu olmalıdır. Yığınlama için kullanıcı veya uplink portları kullanılmamalı ve yığınlama çalıştırıldığında hiç bir kullanıcı portu devre dışı kalmamalıdır.
      19. Anahtar stack modülleri takılı olarak ve en az 0.5m stack kabloları ile teklif edilmelidir.
      20. Anahtar sekiz adete kadar yığınlanabilmelidir.
      21. Tüm yığın tek IP Adresi ve tek bir konfigürasyon üzerinden yönetilebilmeli ve yığın çalışırken yeni bir anahtarı yığına eklenebilmelidir.
      22. Yığında ahtarlama bant genişliği en az 80 Gbps olmalı, yığındaki tüm anahtarlar bu bant genişliğine tam erişime sahip olmalıdır.
      23. Yığındaki farklı anahtarlar üzerinden etherchannel yapmak mümkün olmalıdır. (multi-chassis etherchannel)
      24. Anahtar en az Spanning Tree (802.1d, MST, Rapid), 802.1x, 802.3af, LACP, IGMP Snooping, DHCP Snooping özellikleri için stack yapılmış anahtarlar arasında SSO (Stateful Switchover) desteklemelidir.
      25. L2 Protocols;
      26. Anahtar en az 16.000 adet MAC adresi desteklenmelidir.
      27. IEEE 802.1d Spanning Tree Protocol(STP), 802.1w Rapid Spanning Tree ve 802.1s Multiple Spanning Tree Protocol (MSTP) desteklenmelidir. Vlan’ler arası yük dengelemesi için 802.1d ve 802.1w protokolleri her VLAN için ayrı ayrı çalıştırılabilmelidir.
      28. Anahtar L2 loop’ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.
      29. Anahtar Resilient Ethernet Protokolünü (REP) desteklemelidir.
      30. Fiberoptik arayüzlerde, bağlantıların tek yönlü olarak fiberoptik kablolama veya port hatalarından dolayı arızalanması durumunda bunu algılayan ve tek yönlü olan linkleri kapatan UniDirectional Link Detection(UDLD) özelliği bulunmalıdır.
      31. Anahtarın iki cihaz arasında otomatik olarak L2 trunk oluşturmak için bir protokol desteği bulunmalıdır.
      32. Anahtar IEEE 802.3ad - LACP desteklemelidir. Cihaz üzerinde minimum 8 adet 10/100/1000 ya da 1000BaseX port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.
      33. Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.
      34. L3 Protocols;
      35. Anahtar statik yönlendirme, VLAN’ler arası IP yönlendirme, ve dinamik yönlendirme protokollerinden RIP ve OSPF desteklemelidir.
      36. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir
      37. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.
      38. Anahtar örnekleme yapmadan Netflow veya SFlow desteklemelidir. Üzerinde en az 16.000 adet flow bilgisi tutabilmelidir.
      39. Multicast;
      40. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.
      41. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.
      42. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
      43. Güvenlik;
      44. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
      45. Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
      46. Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden (ACL) geçirebilmelidir. Cihaz üzerinde tanımlanan erişim denetim listeleri zamana bağlı olarak aktif hale getirilebilmelidir.
      47. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
      48. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
      49. Anahtar en az 1500 adet ACL desteğine sahip olmalıdır.
      50. Anahtar her porttan belirlenen adet kadar MAC adresinin bağlantı kurmasını sağlayabilmelidir. Belirlenen limit dışındaki MAC adresleri isteğe bağlı olarak belirlendiğinde port kapatılabilmeli veya limit dışı MAC adreslerinin bağlanması engellenebilmelidir.
      51. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
      52. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilmelidir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).
      53. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapabilmelidir.
      54. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.
      55. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilmelidir.
      56. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.
      57. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
      58. Anahtar hem uplink hem de downlink portlarında 802.1AE, MACSec desteklemelidir.
      59. QoS;
      60. Anahtar Voice VLAN yaratılmasını destekleyecektir. Bu sayede IEEE 802.1p class of service (CoS) uyumlu IP telefonların otomatik olarak tanınması ve Voice Vlan a eklenmesine olanak sağlamalıdır.
      61. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Engress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.
      62. Anahtarın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (IP ToS/DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.
      63. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilmelidir (Rate Limiting).
      64. Management;
      65. Anahtarın IPV4 ve IPv6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.
      66. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPv4 ve IPv6 için desteklenmelidir.
      67. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN) aynalama yeteneği olmalıdır.
      68. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilmelidir.
      69. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
      70. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilek NTP protokolünü desteklemelidir.
      71. Anahtar, SNMP v1, v2c, v3, telnet, Secure Shell (SSH) v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
      72. Anahtar SNMP trap yeteneğine sahip olmalıdır.
      73. En az 4 grup RMON (history, statistics, alarms, events)  desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPv4 hem IPv6 istemcilere servis sağlayabilmelidir.
      74. Cihaz aynı anda 16 adete kadar telnet bağlantısını ve 5 SSH bağlantısını destekleyebilmelidir.
      75. Anahtar 10/100/1000 bakır portlarında TDR (time domain reflector) desteklemelidir. Bu sayede cihaz, bu portlardaki kablolama hatalarını teşhis edebilmeli, kabloda kopukluk olması durumunda ne kadar uzakta olduğunu tespit edebilmelidir.
      76. Anahtar üzerinde yığınlama ekipmanları ve en az 3 metre yığınlama kablosu ile birlikte teklif edilmelidir.
      77. Kenar anahtar, ömür boyu üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile teklif edilecektir.
      78. Anahtar üzerinde en az 1 adet 10GBASE-SR SFP Modül, Enterprise-Class teklif edilecektir. Teklif edilecek modül OEM olmamalıdır. Orijinal ve aynı üreticiye ait olmalıdır.Teklif edilen kenar anahtarlar Omurga anahtar ile aynı üreticiye ait olmalıdır.
      79. Anahtar ile teklif edilen tüm fiber optik modül bağlantıları için en az 2 adet LC-LC, 2 metrelik, Multimode OM3 fiber optik patch kablo teklif edilecektir.
   3. **OMURGA ANAHTARLAR (2 ADET)**
      1. Anahtar üzerinde en az 48 adet 1/10/25Gbps fiber downlink port bulunmalıdır.
      2. Anahtar üzerinde en az 4 adet 40/100Gbps fiber uplink port bulunmalıdır.
      3. Anahtarlama bant genişliği en az 3.2 Tbps olmalıdır.
      4. Anahtarın L2 anahtarlama performans değeri en az 1 Bpps olmalıdır.
      5. Anahtar en az 36 MB buffer’a sahip olmalıdır.
      6. Anahtar IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.
      7. Anahtarın modüler güç kaynağı desteği olmalıdır. İkinci bir dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Anahtarın üzerinde dahili yedek güç kaynağı bulunmalıdır. Yedek güç kaynağı anahtar çalışmaya devam ederken değiştirilebilmelidir.
      8. Anahtar programlanabilir bir ASIC’e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.
      9. Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.
      10. Anahtar 3. parti uygulamaların çalıştırılabileceği bir container altyapısı bulunmalı ve bu altyapıyı destekleyebilecek CPU ve bellek kapasitesi olmalıdır.
      11. Anahtarın işletim sistemi modern programlama dillerinden NETCONF, RESTCONF ve YANG modellerini ve cihaz üzerinde Python scripting desteklemelidir.
      12. Anahtar en az 16Gb DRAM ve 16Gb Flash belleğe sahip olmalıdır.
      13. Anahtar üzerinde en az bir adet USB 3.0 ara yüz bulunmalıdır. Bu arayüz üzerinden anahtara işletim sistemi yüklemek veya log dosyalarını aktarmak mümkün olmalıdır.
      14. Anahtarın 9100 byte’lık jumbo frame desteği olmalıdır.
      15. Anahtar envanter yönetimi için kullanılacak pasif bir RFID etiketine sahip olmalıdır.
      16. Anahtar üzerinde veri merkezi içinde yerinin kolay bulunabilmesi için açılıp kapatılabilen mavi ışık (Blue Beacon) desteğine sahip olmalıdır.
      17. Anahtar yazılımsal olarak Bluetooth desteğine sahip olmalıdır. Opsiyonel olarak bağlanacak bluetooth aparatı üzerinden anahtarın WEB ve komut arayüzüne erişmek, log ve işletim sistemi transferi yapmak mümkün olmalıdır.
      18. Virtual Stack;
      19. İki anahtar portları üzerinden birbirine bağlanarak, sanal olarak tek anahtar olarak çalışabilmeli ve tek IP erişimi ile yönetilebilmelidir. Bu yapıda sanal olarak birleştirilmiş anahtarlar MCEC (Multi-chassis EtherChannel) desteklemelidir.
      20. L2 Protocols;
      21. Anahtar en az 82.000 adet MAC adresi desteklenmelidir.
      22. En az 4000 adet aktif VLAN desteği olmalıdır.
      23. IEEE 802.1d Spanning Tree Protocol(STP), 802.1w Rapid Spanning Tree ve 802.1s Multiple Spanning Tree Protocol (MSTP) desteklenmelidir. Vlan’ler arası yük dengelemesi için 802.1d ve 802.1w protokolleri her VLAN için ayrı ayrı çalıştırılabilmelidir.
      24. Anahtar L2 loop’ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.
      25. Anahtar Resilient Ethernet Protokolünü (REP) desteklemelidir.
      26. Fiberoptik arayüzlerde, bağlantıların tek yönlü olarak fiberoptik kablolama veya port hatalarından dolayı arızalanması durumunda bunu algılayan ve tek yönlü olan linkleri kapatan UniDirectional Link Detection özelliği bulunmalıdır.
      27. Anahtarın iki cihaz arasında otomatik olarak L2 trunk oluşturmak için bir protokol desteği bulunmalıdır.
      28. Anahtar IEEE 802.3ad-LACP desteklemelidir. Cihaz üzerinde minimum 8 adet 10/100/1000 ya da 1000BaseX port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.
      29. Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.
      30. L3 Protocols;
      31. Anahtar en az 212.000 adet IPv4 ve IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.
      32. Anahtar statik yönlendirme, VLAN’ler arası IP yönlendirme, ve dinamik yönlendirme protokollerinden en az RIP ve OSPF desteklemelidir.
      33. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir
      34. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.
      35. Anahtar örnekleme yapmadan Netflow veya SFlow desteklemelidir. Üzerinde en az 64.000 adet flow bilgisi tutabilmelidir.
      36. Multicast;
      37. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.
      38. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.
      39. Anahtar en az 16.000 adet IGMP snooping girdisi desteklemelidir.
      40. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
      41. Güvenlik;
      42. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
      43. Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
      44. Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden (ACL) geçirebilmelidir. Cihaz üzerinde tanımlanan erişim denetim listeleri zamana bağlı olarak aktif hale getirilebilmelidir.
      45. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
      46. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
      47. Anahtar en az 5000 adet ACL desteğine sahip olmalıdır.
      48. Anahtar her porttan belirlenen adet kadar MAC adresinin bağlantı kurmasını sağlayabilmelidir. Belirlenen limit dışındaki MAC adresleri isteğe bağlı olarak belirlendiğinde port kapatılabilmeli veya limit dışı MAC adreslerinin bağlanması engellenebilmelidir.
      49. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
      50. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilmelidir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).
      51. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapabilmelidir.
      52. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.
      53. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilmelidir.
      54. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.
      55. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
      56. Anahtar hem uplink hem de downlink portlarında 802.1AE, MACSec desteklemelidir.
      57. QoS;
      58. Anahtar Voice VLAN yaratılmasını destekleyecektir. Bu sayede IEEE 802.1p class of service (CoS) uyumlu IP telefonların otomatik olarak tanınması ve Voice Vlan a eklenmesine olanak sağlamalıdır.
      59. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Engress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.
      60. Anahtarın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (IP ToS/DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.
      61. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilmelidir (Rate Limiting).
      62. Management;
      63. Anahtarın IPV4 ve IPv6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.
      64. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPv4 ve IPv6 için desteklenmelidir.
      65. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN) aynalama yeteneği olmalıdır.
      66. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilmelidir.
      67. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
      68. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilek NTP protokolünü desteklemelidir.
      69. Anahtar, SNMP v1, v2c, v3, telnet, Secure Shell (SSH) v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
      70. Anahtar SNMP trap yeteneğine sahip olmalıdır.
      71. En az 4 grup RMON (history, statistics, alarms, events)  desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPv4 hem IPv6 istemcilere servis sağlayabilmelidir.
      72. Cihaz aynı anda 16 adete kadar telnet bağlantısını ve 5 SSH bağlantısını destekleyebilmelidir.
      73. Anahtar L3 statik yönlendirme ve IPv4 ve IPV6 dinamik yönlendirme protokollerinden RIP, RIPng, OSPF, OSPFv3, BGP, multiprotocol BGP ve IS-IS desteklemelidir.
      74. Anahtar OSPF ve BGP protokolleri için NSF (non-stop forwarding) desteklemelidir.
      75. Anahtar NAT (Network Address Translation), PAT (Port Address Translation) desteklemelidir.
      76. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtar port aynalama yöntemlerinden SPAN, RSPAN ve ERSPAN özellikleri olmalıdır.
      77. Anahtar anormallik tespti yapabilen sistemler tarafından kullanılmak üzere, şifrelenmiş trafiklerle ilgili, şifrelemeyi açmadan analitik bilgiler oluşturabilmeli ve netflow paketleri üzerinden paylaşabilmelidir.
      78. Anahtar en az 1400 adet uygulamayı tanıyabilmeli, bu bilgileri QoS tanımlarında kullanabilmeli, anahtar üzerinde raporlayabilmeli veya netflow üzerinden yönetim sistemleriyle paylaşabilmelidir.
      79. Anahtarın işletim sistemi yazılım seviyesini değiştirmeden belli hataları düzeltmek için üretilen yamalama (Patch) yeteneğine sahip olmalıdır.
      80. Anahtar Wireshark desteğine sahip olmalıdır. Anahtar üzerindeki herhangi iki port arasındaki trafik yakalanıp yine anahtar üzerinde paket paket incelenebilmeli veya Wireshark uygulaması kurulu bir sisteme gönderilebilmelidir.
      81. Anahtar HSRP üçüncü katman yedekleme protokolünü desteklemelidir.
      82. Anahtar en az 32.000 adet IPv4 ve IPv6 multicast route kapasitesine sahip olmalı ve L3 multicast protokollerinden en az PIM-Sparse, Bidirectional PIM (PIM-BiDir), Source-Specific Multicast (SSM) ve Multicast Source Discovery Protocol (MSDP) desteği bulunmalıdır.
      83. Anahtar hem uplink hem de downlink portlarında AES-256 tabanlı 256-bit 802.1AE, MACSec desteklemelidir.
      84. Anahtar VRF-lite, L3-MPLS-VPN, L2VPN (EoMPLS, VPLS) ve GRE desteklemelidir.
      85. Anahtar bir uç noktaya olan erişimin kalitesini (paket kaybı, gecikme, jitter) ölçmek için IP SLA desteğine sahip olmalıdır.
      86. Omurga anahtar, ömür boyu üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile teklif edilecektir.
      87. Anahtar üzerinden en az 3 adet 100GBASE PSM4 QSFP Transceiver, MPO, 500m over SMF, en az 6 adet 10GBASE-SR SFP Modül, en az 5 adet 1G Bakır SFP modül ve en az 5 adet 1000BASe-SX MM SFP teklif edilecektir. Teklif edilecek modül OEM olmamalıdır. Orijinal ve aynı üreticiye ait olmalıdır. Teklif edilen kenar anahtarlar Omurga anahtar ile aynı üreticiye ait olmalıdır.
      88. Anahtar ile teklif edilen tüm fiber optik modül bağlantıları için en az 6 adet 40/100 Gbps F/O MPO Female to MPO Female 5 metre fiber patch kablo, en az 10 adet 1 metre Cat.6 UTP LSZH Patch kablo teklif edilecektir.
   4. **KABLOSUZ AĞ KONTROL CİHAZI (2 ADET)**
      1. Teklif edilen Kablosuz Denetleyici bu şartnamede teklif edilecek kablosuz bağlantı noktalarını yönetecektir.
      2. İstenilen Kablosuz Denetleyici ek bir cihaz, parça veya karta ihtiyaç olmadan en az 250 adet lokal ağa bağlı kablosuz erişim noktasına aynı anda hizmet verebilecektir.
      3. 5000 adet son kullanıcıya kadar destek verecektir.
      4. Kablosuz Denetleyici N+1 yedekliliği desteklemelidir, aktif denetleyicinin devre dışı kalması durumunda üzerindeki kullanıcılar ve oturumları kayıp yaşanmadan yedek denetleyiciye aktarılabilmelidir.
      5. Kablosuz Denetleyici N+1 yedekliliği desteklemelidir, aktif denetleyicinin devre dışı kalması durumunda üzerindeki kablosuz erişim noktaları (Access Point) oturum kaybı yaşanmadan yedek denetleyiciye aktarılabilmelidir.
      6. Kablosuz Denetleyici en az 5 Gbps throughput değerine sahip olmalıdır. Kablosuz denetleyicinin sağladığı en yüksek throughput değeri, üzerinde eğer varsa firewall servisleri açılınca herhangi bir düşüşe uğramamalıdır.
      7. Kablosuz Denetleyici, IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac standartlarını destekleyecektir.
      8. Kablosuz denetleyici ayrıca IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q Vtagging, and IEEE 802.1AX Link Aggregation kablolu ağ protokollerini desteklemelidir.
      9. Kablosuz Denetleyici DTLS detekleyecektir. Kablosuz Denetleyici ile erişim noktası arasındaki trafik şifreli ve güvenli olmalıdır. Bu özellik erişim noktası WAN veya LAN bağlantısı fark etmeksizin kullanılabilir olmalıdır.
      10. Kablosuz Denetleyici ve bağlı olduğu donanım/yazılımlar ile tüm kablosuz erişim noktalarının kanal, çıkış gücü gibi ayarlamalarını otomatik yapılmalı, değişen koşullara, sinyal gürültü durumlarına, ortamdaki yabancı kablosuz ağ donanımlarına göre çıkış gücü ve kanalları otomatik değiştirebilmelidir. Ortamda mikrodalga, bluetooth gibi enterferans kaynakları varsa, Kablosuz Denetleyici bunu tespit ederek, kablosuz erişim noktalarını farklı kanallara otomatik atayabilmelidir.
      11. Aynı kapsama alanında bir kablosuz erişim noktasının servis vermemesi, diğer cihazlar tarafından fark edilebilmeli, komşu cihazlar otomatik olarak yayın güçlerini artırıp servis vermeyen kablosuz erişim noktasından kaynaklı RF kapsama boşluğunu azaltmaya çalışmalıdır.
      12. Kablosuz Denetleyici ve bağlı olduğu donanım/yazılımlar ile aynı kapsama alanına hizmet veren iki kablosuz erişim noktası arasında kullanıcılara yük paylaşımı yapabilmelidir. Bu yük paylaşımı, kullanıcı sayısına göre ayarlanabilmelidir.
      13. Kablosuz Denetleyici, tüm kablosuz ağ trafiğini kendi üzerinden geçirecek şekilde tasarlanmış olmalıdır.
      14. İstenmesi durumunda Kablosuz Denetleyici erişim noktalarını sadece yönetmeli ve trafiği kendi üzerinden geçirmeden de kablosuz ağ yapısı kurabilmelidir. Bu işlemi WAN bağlantısı üzerinden uzak ofisler için de yapabilmelidir. Olası WAN bağlantısının kesilmesi durumunda erişim noktaları o anki çalışmalarına devam edebilmelidir. WAN bağlantısı sağlanamadığı süre içinde, uzak erişim noktaları üzerlerine yeni kullanıcı alma, erişim noktaları arasında roaming, varsa lokaldeki radius server yetkilendirmesi ve varsa lokal portal erişimi işlemlerinin tamamı yapılabilmelidir. Bu işlemler için gereken donanım, yazılım ve lisanslar teklife dahil edilecektir. Bu özelliğin tanımlanan biçimde yapılamaması durumunda eşdeğer özelliklerde en az 1 adet ek kablosuz denetleyici daha teklif edilecektir.
      15. Kablosuz Denetleyici, uyumlu erişim noktaları arasında mesh yapı kurulumu ve yönetimini destekleyecektir.
      16. Kablosuz Denetleyici en az 4096 WLAN ve en az 4096 VLAN destekleyecektir. Cihaz tekbir SSID’ye bağlanan kullanıcıları birden fazla farklı VLAN lara yönlendirebilecektir.
      17. Kablosuz Denetleyici üzerinde, belli bir anda hangi tipte/modelde kaç kablosuz erişim noktasının sisteme bağlı olduğunu görülebilmelidir.
      18. Kablosuz Denetleyici, birden fazla bantta farklı MAC adresleriyle yayın yapan kablosuz erişim noktalarını tek bir kablosuz erişim noktası şeklinde gösterebilmelidir.
      19. Kurulacak sistemde, bir kullanıcının bir kablosuz erişim noktasının kapsama alanından diğer bir kablosuz erişim noktasının kapsama alanına geçerken hissetmeyeceği şekilde bağlantıyı devam ettirecek “mobility” özelliği bulunmalıdır.
      20. Kablosuz Denetleyici ile misafir kullanıcılara bir web arayüzü çıkartarak buradan yetkilendirme yapılması mümkün olmalıdır. İsteklinin önereceği markaya ait donanım/yazılımlarda, misafir kullanıcılara değişik haklar ve sınırlamalar tanımlanabileceği bir çözüm sunulabilmelidir. (belli bir VLAN’a atama, belli bir süre sistemi kullanma, belli IP bloklarına erişim vs.). Kullanıcıya çıkacak web arayüzü İdare tarafından özelleştirilebilmeli, gerektiğinde harici bir başka web sunucuya yönlendirilebilmelidir. Kullanıcılara çıkartılacak web ara yüzünden girilecek şifre bilgileri, İdarenin kullandığı Radius /Ldap sunucuları üzerinden yetkilendirilebilmelidir.
      21. Tüm kablosuz erişim noktalarının yazılım sürümü merkezi olarak denetlenebilmelidir. Yeni bir yazılım, Kablosuz Denetleyiciye eklendiği anda, otomatik olarak tüm ağ cihazlarına aynı anda veya gruplar halinde yazılım yükseltmesi yapılabilmelidir.
      22. Kablosuz Denetleyici, Telnet, SSH, http ve https protokolleri kullanılarak yönetilebilmelidir.
      23. Kablosuz Denetleyici entegre bir DHCP sunucu desteği sağlayacaktır.
      24. Kablosuz Denetleyicinin, IPv6 protokol desteği olmalıdır. Kablosuz Denetleyici, IPv6 adresine sahip kullanıcılara hizmet verebilmelidir.
      25. Kablosuz denetleyicinin QoS desteği olmalıdır. QoS politikaları erişim noktasına, yayınlanan SSID’ye 2.4 / 5 GHz bandına yapılabilmelidir. Adil bant genişliği ataması yapılabilmelidir.
      26. Kablosuz Denetleyici ek bir donanım veya yazılıma ihtiyaç duymadan entegre bir uygulama tanıma sistemi barındırmalıdır. Cihaz kendi üzerinden geçen trafiğe derin paket inceleme
      27. (Deep Packet Inspection) tekniklerini uygulayarak 1000’in üzerinde uygulamayı tanıyabilmelidir. Sınıflandırdığı uygulamalara QoS atayabilmeli ve bant genişliği belirtebilmelidir.
      28. Tanınan uygulamalar için yapılan QoS işlemi teklif verilirken açıklanmalı ve QoS ve/veya rate limiting parametreleri, en az paket boyutu gibi değerler belirtilmelidir. Ayrıca uygulama tanıma özelliği ile ilgili geçmişe dönük raporlar alınabilmelidir. Eğer bu özellik tanımlandığı biçimde desteklenmiyorsa eşdeğer özelliklerde en az 1 adet ek koblosuz denetleyici daha teklif edilecektir.
      29. İstenildiğinde kablosuz ağ trafik analizi yapılabilmesi amacı ile WLC netflow veya sflow desteği sağlamalıdır.
      30. Kurulacak Kablosuz Ağ Sistemi WPA2-Enterprise (802.1X kullanımı için) uyumlu olmalıdır. Tüm EAP (EAP-TTLS gibi) tiplerinin sorunsuz olarak çalışmasını desteklemelidir.
      31. Merkezi yönetim işlerinde kullanılan tüm donanımların üzerinde takılı olan flash disk ve hafızalar donanımsal olarak desteklenen en üst kapasitede ve hızda olacaktır.
      32. Kablosuz Denetleyici, kendisine bağlı AP'lerin, ortamdaki en uygun kanalı belirlemek için yaptığı RF taramalar sırasında, ortamda yüksek yoğunlukta trafik oluşturan kullanıcılar varsa, RF tarama özelliğini erteleyebilmelidir.
      33. Havayı gerçek zamanlı izleyip, birinci katmanda RF analizi yapabilme modulu olmalıdır
      34. WLC sistem dışı (rogue) AP’larının sistem yöneticisi tarafından tanımlanan kurallarla tespitine ve bu AP’larına kullanıcıların bağlanmasının engellenerek etkisizleştirilmelerine olanak sağlamalıdır.
      35. Kablosuz denetleyici, ek bir yazılım veya donanıma ihtiyaç duymadan entegre biçimde wIDS (kablosuz saldırı tespit sistemi) barındırmalıdır.
      36. Cihaz üzerinde en az 4 adet 1 / 2,5 Gb Ethernet modül yuvası ve USB 3.0 bağlantı ara yüzü olacaktır. 2 adet 10G SFP Modül yuvaları olacaktır. İstenmesi durumunda 10G Modül yuvaları 1G hızında da kullanılabilmelidir.
      37. Teklif edilecek ürünün tüm aksesuarları (kabin montaj kiti, konsol kablosu, vida v.s) ile teklif edilecektir.
      38. Tespit edilen problemlerle ilgili çözüm önerileri sunabilmeli, problem çözümü için uygulanacak ek işlemler için alternatifler sunabilmelidir.
      39. Ağ cihazlarının CPU, Bellek ve portlarındaki trafik kullanım ve paket kayıp/hata oranlarını grafiksel olarak gösterebilmelidir.
      40. Sistemin REST API desteği olmalı ve üçüncü parti uygulama ve yazılımlarla entegre edilebilmelidir.
      41. Sistemin Ağ Erişim Kontrol Sistemi ile entegrasyonu olmalıdır.
      42. Sistemin yöneticileri için rol tabanlı erişim yetkileri tanımlamak mümkün olmalıdır.
      43. Sistem VXLAN kullanılan yazılım tabanlı (Software-Defined) bir üst katman yapının otomasyonunu desteklemelidir. Teklifte bu istenmemekte olup; talep edildiğinde yazılım yükseltmesi ya da lisans alımı ile sağlanabilmelidir.
      44. Teklif edilen ürün, yedekli çalışabilmesi için gerekli lisanslar ile teklif edilecektir.
      45. Teklif edilen ürün, ömür boyu üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile teklif edilecektir.
   5. **İÇ ORTAM KABLOSUZ YAYIN CİHAZI (120 ADET)**
      1. Önerilecek olan kablosuz ağ erişim cihazı (kablosuz erişim noktası), çift radyolu olmalı ve ETSI standartlarında 2.4 GHz ve 5 GHz frekans bandında çalışabilmelidir. Cihaz akıllı bir algoritma sayesinde, içinde bulunduğu RF ortamına göre aşağıda belirtilen farklı modlar da çalışabilmelidir:
      2. a. 2.4 ve 5 GHz modunda, radyolardan birinden 2.4 ve diğerinden 5 GHz kanalında istemcilere yayın yapabilmelidir.
      3. b. Cihaz Dual 5 GHz modunda, üzerinde bulunan iki radyodan da 5 GHz kanalında istemcilere yayın yapabilmelidir.
      4. Kablosuz erişim noktası, teklif edilen merkez kablosuz ağ kontrol cihazı tarafından yönetilebilmelidir. Kablosuz erişim noktası üzerindeki kullanıcı trafiği, merkez kablosuz ağ kontrol cihazı üzerinden ağa iletilmelidir.
      5. Kablosuz erişim noktası, IEEE 802.11n, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, 802.11ac Wave 2 ve 802.11ax standartlarını uyumlu olarak destekleyecektir.
      6. Kablosuz erişim noktası, ETSI standartlarının (2,4 ve 5 GHz) izin verdiği sayıda erişim noktası ile, aynı ortamda yan yana frekans örtüşmesi olmadan çalışacaktır.
      7. Cihaz üzerindeki kullanıcılar 802.11n standardında 600 Mbps, 802.11ac standardında 3,4 Gbps, 802.11ax standardında 4,8 Gbps hıza ulaşabilmelidir.
      8. 802.11ax standartı özelliklerinden OFDMA, Target Wake Time ve BSS Coloring desteklenecektir.
      9. Kablosuz erişim noktası 802.11 dynamic frequency selection (DFS), maximal ratio combining (MRC), cyclic shift diversity (CSD) ve 20, 40, 80 ve 160 MHz kanallarını desteklemelidir.
      10. Kablosuz erişim noktası, 4x4 MU-MIMO (MultiUser - Multiple Input Multiple Output)’u desteklemelidir. Erişim noktası; en az 4 uzaysal akışı (spatial stream) destekleyecektir.
      11. Kablosuz erişim noktası üzerinde en az 1 adet 100, 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz port bulunacaktır.
      12. AP üzerinde 2,4 GHz için kazanımı en az 4 dBi ve 5 GHz için kazanımı en az 5 dBi olan entegre dahili antenler bulunmalıdır.
      13. AP üzerinde en az 1 adet lokal yönetim amaçlı RJ-45 konsol portu bulunacaktır.
      14. Kablosuz erişim noktası, IEEE 802.3af (PoE), 802.3at (PoE+) ve 802.3bt (UPoE) ile UTP kablo üzerinden beslenebilmelidir. PoE+ ve UPoE kullanılması durumunda wireless özellikleri tam kapasite ile çalışabilmelidir.
      15. AP üzerinde IoT uygulamaları için Bluetooth Low Energy (BLE) desteği bulunmalıdır.
      16. 5GHz desteği bulunan istemcileri eğer istenirse 5GHz bandında çalışmaya zorlayabilmelidir.
      17. Cihaz Kablosuz saldırı engelleme sistemelerinin sensoru şeklinde çalışabilecektir. Kapsama alanı içinde bulunan kuruma ait olmayan kablosuz erişim noktalarını da tespit edebilecektir. Aynı anda hem saldırı engelleme sensoru olarak çalışabilmeli hem de istemcilere hizmet verebilecektir.
      18. Cihaz kullanıcıları kesintisiz ve sorunsuz video yayın alabilmesi için multicast video yayınını unicast olarak kullanıcılara gönderebilmelidir ve bu trafigi kablosuz erişim noktası üzerinde unicast’e çevirmelidir. Merkezi kontrol cihazı ile unicast’e çevrilen çözümler kabul edilmeyecektir.
      19. Cihazın çıkış gücü (transmit power), ETSI standartlarına uygun olmalıdır. Çıkış gücü, standarlar içerisinde farklı seviyelere ayarlanabilmelidir.
      20. Kablosuz erişim noktası, Wi-Fi Protected Access (WPA) ve WPA2 sertifikasyon yöntemlerini desteklemelidir. WPA2 için AES (advanced encryption standart) şifreleme desteği bulunmalıdır. Kablosuz erişim noktası, IEEE 802.11i güvenlik standartını desteklemelidir.
      21. Kablosuz erişim noktası, IEEE 802.1x authentication desteğine sahip olmalıdır.
      22. Kablosuz erişim noktası üzerinde, cihazın durumunu, ethernet bağlantısının durumunu ve aktivitesini, kablosuz bağlantının durumunu ve aktivitesini gösteren LED veya LED ler bulunmalıdır.
      23. Cihazın duvara, tavana ya da masa üstüne monte edilmesini sağlayan kitler birlikte verilecektir.
      24. Teklif edilen ürün, ömür boyu üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile teklif edilecektir.
      25. Teklif edilen ürün, kablosuz ağ kontrol cihazı ile aynı üreticiye ait olmalıdır.
   6. **NETWORK YÖNETİM YAZILIMI**
      1. Kurumun bünyesindeki router, switch, access point ve controller cihazlarının tek bir noktadan merkezi yönetimi, izlenmesi ve sorun giderme işlemleri için bir urun teklif edilecektir.
      2. Tüm bu cihazlar tek bir yönetim merkezi tarafından yönetilemiyorsa, ayrı ayrı yönetilmesini sağlayan tüm yönetim yazılımları gerekli lisanslarla teklif edilmelidir.
      3. Yazılım switchleri ve ortamdaki kablosuz erişim noktalarını otomatik bulabilmelidir.
      4. Tüm switch’lerin konfigürasyonunu uzaktan güvenli bir şekilde yapabilmeli, yedeğini alabilmelidir.
      5. Temel ağ arıza bulma verilerini oluşturarak raporlayabilmelidir.
      6. Geriye dönük rapor alabilmelidir.
      7. Cihazların durumu hakkında bilgi vermelidir. Ulaşılabilirlik, kaynak kullanımı, port durumu vs. gibi bilgileri gösterebilmelidir.
      8. Yazılım sistem arıza analizinde kullanım için veri üretebilmeli, tanımlanan eşik değerleri için alarm üretebilmelidir.
      9. Ağ yönetim yazılımı cihazlara zamanlanmış konfigürasyon yapabilmelidir.
      10. Ağ yönetim yazılımı üzerinden üreticinin teknik destek ekiplerine case açılabilmeli ve destek forumlarına erişilebilmelidir.
      11. Yazılım ağ topolojisini otomatik olarak oluşturabilmeli ve elle ekleme veya değişiklik yapılmasına da izin vermelidir.
      12. Yazılım ağdaki trafiği analiz etme amaçlı netflow toplama işlemi yapabilmelidir ve uygulama katmanında trafik gösterebilmelidir.
      13. Yazılım üreticinin ürünlerindeki çeşitli özelliklerin (örneğin Uygulama Görünürlüğü ve Kontrolü) yapılandırılması için taslaklar sunmalıdır.
      14. Yazılım controller ile entegre olup ortamdaki yabancı erişim noktalarının bağlı olduğu switch port’larini tespit edebilmelidir.
      15. Teklif edilen yazılım, en az 350 adet Access point, en az 158 adet switch ürünlerinin lisansları da dahil edilecektir.
      16. Teklif edilen yazılım, kenar anahtarlar, kablosuz ağ yönetim sistemi ve omurga anahtarlar ile aynı üreticiye ait olmalıdır.
   7. **KABLOSUZ AĞ KONTROL CİHAZI (2 ADET)**
      1. Teklif edilen merkez kablosuz ağ kontrol cihazı ve erişim noktası cihazları aynı üreticiye ait olmalıdır.
      2. Teklif edilen kablosuz erişim cihazlarının merkezi yönetimi için kullanılacaktır.
      3. Cihazın AC güç kaynağı dahili olarak yedeklenebilecektir ve yedekli olarak teklif edilecektir.
      4. Cihaz, en az 2000 adet lokal erişim noktası cihazını destekleyecek donanım yapısına sahip olacak şekilde teklif edilecektir.
      5. Cihaz, en az 32000 kullanıcıyı destekleyecek donanım yapısına sahip olacak şekilde teklif edilecektir.
      6. Cihaz, en az teklif edilen lokal erişim noktası adedini destekleyecek lisanslama ile teklif edilecektir.
      7. Kablosuz ağ kontrol cihazı üzerinde en az 4 adet 10GBaseX port bulunacaktır.
      8. En az 40 Gbps throughput sağlamalıdır.
      9. En az 4096 kablosuz ağı desteklemelidir.
      10. En az 4096 VLAN desteklemelidir.
      11. Kablosuz ağ kontrol cihazı üzerinde yönetim amaçlı en az 1 adet 10/100/1000 Mbps Ethernet port ve konsol bağlantısı için bir adet konsol portu bulunacaktır.
      12. Cihaz, RF girişim etkilerine karşı, tespit etme ve önleme özelliklerine sahip olmalıdır.
      13. Cihaz, erişim noktaları arasında yük paylaşımı yaptırabilmelidir.
      14. Cihaz ağın durumuna göre, erişim noktalarının RF çıkış gücünü, dinamik ve gerçek zamanlı olarak ayarlayabilmelidir.
      15. Eğer bir erişim noktası çalışamaz duruma gelirse, cihaz diğer erişim noktalarında gerekli güç ve RF değişikliklerini yaparak çalışmayan erişim noktasının alanını kapsayabilmelidir.
      16. Cihaz IEEE 802.11ac, 802.11ac wave2 ve 802.11ax standartlarını destekleyecektir.
      17. IEEE 802.1X standardını desteklemelidir. IEEE 802.1X desteği olmayan istemciler için web tabanlı yetkilendirme yapabilmelidir.
      18. Misafir VLAN desteği olmalıdır. IEEE 802.1X yetkilendirmesinde başarısız olan istemcileri, otomatik olarak kısıtlı bir VLAN’a atayabilmelidir.
      19. WPA, WPA2 ve WPA3 desteği olmalıdır.
      20. Harici bir RADIUS ve/veya TACACS sunucusu üzerinden, kullanıcıların kimlik sorgulamasını yapabilmelidir.
      21. Kablosuz ağ kontrol cihazı, istenmesi durumunda N+1 modunda yedekli çalışmayı desteklemelidir.
      22. Kablosuz ağ kontrol cihazında herhangi bir arıza olması durumunda, kendisine bağlı olan kablosuz erişim noktaları, otomatik olarak aynı ağ kontrol cihazı grubunda bulunan, 1 veya daha fazla kablosuz ağ kontrol cihazına kaydolmalıdır.
      23. Kablosuz ağ kontrol cihazı, uzak bölgelerde bulunan erişim noktalarını yönetebilmelidir.
      24. Teklif edilen kablosuz ağ kontrol cihazı ve erişim noktaları, uzak bölgelerde bulunan kullanıcıların, birbirleri arasındaki trafiği, merkez kablosuz ağ kontrol cihazına taşımadan yerel olarak anahtarlanmasını sağlamak için, “local switching” (H-Reap.. vb) protokollerinden en az birini desteklemelidir. Aynı zamanda uzak bölgede bulunan erişim noktaları ile merkez kablosuz ağ kontrol cihazının bağlantısı kesildiğinde, erişim noktaları, yerel alan ağına hizmet vermeye devam edebilmelidir. Desteklenen protokol belirtilecektir.
      25. Aynı lokasyondaki yedekli ağ kontrol cihazlarından bir tanesinin düşmesi durumunda erişim noktalarının tekrar tünel kurması veya client’ların yeniden authenticate olması gerekmemelidir. Bir ağ kontrol cihazından diğer ağ kontrol cihazına geçiş birkaç saniye içerisinde gerçekleşebilmelidir.
      26. BYOD için kablosuz cihazları ve uygulamaları (7. katmanda) ayrımlayabilmeli; önceden belirlenmiş VLAN etiketi, servis kalitesi kuralları, erişim kuralları, saat bazlı erişim gibi politikaları uygulatabilmelidir. Bunun için cihaz üzerinde verilmesi gereken ek lisans varsa teklife dahil edilecektir.
      27. Layer 2 komşuluğu bulunan kablosuz erişim noktalarında Bonjour servisini algılayabilmelidir.
      28. Video Stream desteği bulunmalıdır: sekiz seviyeli önceliklendirme ile kritik video uygulamalarını ayırt edebilmelidir, band genişliğini daha etkiili kullanmak üzere video için olan multicast trafiği unicasta çevirebilmeli, böylelikle sadece ilgili AP ve Clientların alması sağlanabilmelidir.
      29. Ek kablosuz erişim noktası lisansı eklendiğinde cihaz yeniden başlatılmadan bu lisansları kullanmaya başlayabilmelidir.
      30. Belli kablosuz erişim noktaları gruplanarak bu gruplara RF profilleri atanabilmelidir.
      31. 802.11r Fast Transitioning standardını desteklemelidir.
      32. 802.11w Management Frame Protection özelliğini desteklemelidir.
      33. Kimlik denetimi yapılmayacak şekilde yapılandırılan kablosuz ağlarda EAP isteklerini harici bir kimlik denetimi sunucusuna yönlendirebilmelidir.
      34. Üreticinin kimlik servisleri çözümüyle birlikte çalışıp cihazları ağa kaydedebilmeli ve cihazlara servis sağlayabilmelidir.
      35. DHCP isteklerinden istemci ağ adını ve üreticiyi belirleyebilmelidir.
      36. Kablosuz ağ bazında MAC adres bazlı statik WEP kimlik denetimine ek olarak 802.1X kimlik denetimi de yapabilmelidir.
      37. Aynı kablosuz ağda hem 802.1X hem de web kimlik denetimi yapabilmelidir.
      38. Hem indirme hem de yükleme trafiğine rate limiting uygulanabilmelidir. Rate limiting SSID başına veya tüm istemcilere uygulanabilmelidir. Rate limiting hem lokal modda hem de flex connect modunda uygulanabilmelidir.
      39. Cihaz DHCP isteklerine option 82 bilgisi ekleyebilmelidir.
      40. Teklif edilen ürün, ömür boyu üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile teklif edilecektir.
   8. **MASA IP TELEFON TİP- 1 (90 ADET)**
      1. Ayrı bir PBX ve telefon kablolaması yatırımı olmadan, varolan data altyapısı ve data hatları kullanılarak çalışabilmelidir.
      2. Telefonun üzerinde, LAN ve PC bağlantısı sağlamak amacıyla 2 x 10/100/BaseT portlu ethernet switch bulunmalıdır. Bu switch, IEEE 802.1Q VLAN trunking protokolünü desteklemelidir.
      3. Telefona, AC –48 V DC adaptör ile ya da Ethernet kablosu üzerinden IEEE 802.3af Class 1 PoE standardı ile elektrik verilebilmelidir.
      4. Cihaz üzerinde en az 2 yönlü navigasyon butonu olmalıdır.
      5. Telefon, G.722, G.711, G.729a, ve iLBC ses sıkıştırma algoritmalarını desteklemelidir. LAN ve WAN çağrılarında farklı codec kullanılabilmelidir.
      6. Telefonun en az 3.2 inch ve en az 384 x 106 çözünürlükte LCD ekranı olmalıdır.
      7. Kullanıcılar, ahizeyi kaldırmadan karşı tarafla konuşabilmelidir (hands-free speakerphone özelliği olmalıdır).
      8. Telefonun mikrofonu sessiz (mute) moduna alınabilmelidir.
      9. Kullanıcılar; zil seslerini, ahizeden, ya da hoparlörden duyulan ses düzeyini kendileri ayarlayabilmelidir.
      10. Telefon, DHCP sunucudan IP adresini kendisi alabilmeli ya da statik IP adresi ile konfigüre edilebilmelidir. Telefon, otomatik olarak çağrı yöneticisine kayıt olabilecek ve TFTP sunucudan konfigürasyon bilgilerini alabilecektir. TFTP ile firmware güncellemesi yapılabilecektir.
      11. Uzak noktalardaki telefonlar, merkez noktadaki çağrı yöneticisi ile çalışabilmelidir. Telefonlar, WAN hatlarındaki bir kopukluk durumunda yedekli çalışmayı desteklemelidirler.
      12. Telefon, XML (Extensible Markup Language) uygulamalarını desteklemelidir.
      13. Telefon masa üstünde durabileceği gibi, duvara da monte edilebilmeyi desteklemelidir.
      14. Ekran üzerinde cevapsız çağrılar, arayan isim ve numara, arama süresi, tarih ve zaman bilgileri gösterilecektir.
      15. SIP tabanlı haberleşmeyi desteklemelidir.
      16. Telefon üzerinde sabit çağrı bekletme, transfer ve konferans tuşu bulunmalıdır.
      17. Telefon üzerinden tek bir tuş yardımı ile kurumsal rehbere ve sesli mesaj servisine erişim mümkün olabilmelidir.
      18. Telefon, çağrı bekletme (call hold), çağrı aktarma (call transfer), çağrı yönlendirme (call forward), aynı hattan ikinci çağrıyı alabilme (call waiting), üçlü ya da daha çok kişiyle görüşme (conference), tek tuşla arama (speed dial), çağrı parketme (call park), çağrı çekme (call pick-up) özelliklerini desteklemelidir.
      19. Telefon ile çağrı yöneticisi arasında, sayısal sertifikalar aracılığı ile kimlik doğrulaması ve şifreli haberleşme yapılabilmelidir.
      20. Telefon ile diğer güvenli haberleşmeyi destekleyen telefonlar arasında şifreli görüşmeler (authenticated and encrypted calls) yapılabilmelidir.
   9. **MASA TLEFONU TİP -2 (1 ADET)**
      1. Ayrı bir PBX ve telefon kablolaması yatırımı olmadan, varolan data altyapısı ve data hatları kullanılarak çalışabilmelidir.
      2. Telefonun üzerinde, LAN ve PC bağlantısı sağlamak amacıyla 2 x 10/100/BaseT portlu ethernet switch bulunmalıdır. Bu switch, IEEE 802.1Q VLAN trunking protokolünü desteklemelidir.
      3. Telefona, AC –48 V DC adaptör ile ya da Ethernet kablosu üzerinden IEEE 802.3af Class 1 PoE standardı ile elektrik verilebilmelidir.
      4. Bir telefona 16 adede kadar dahili hat numarası verilebilmelidir.
      5. Cihaz üzerinde en az 4 adet programlanabilir tuş bulunmalıdır.
      6. Cihaz üzerinde en az 2 yönlü navigasyon butonu olmalıdır.
      7. Telefon, G.722, G.711, G.729a, ve iLBC ses sıkıştırma algoritmalarını desteklemelidir. LAN ve WAN çağrılarında farklı codec kullanılabilmelidir.
      8. Telefonun en az 3.5 inch ve en az 396 x 162 çözünürlükte arkadan aydınlatmalı LCD ekranı olmalıdır.
      9. Telefonun kulaklık (headset) girişi olmalıdır.
      10. Kullanıcılar, ahizeyi kaldırmadan karşı tarafla konuşabilmelidir (hands-free speakerphone özelliği olmalıdır).
      11. Telefonun mikrofonu sessiz (mute) moduna alınabilmelidir.
      12. Kullanıcılar, ekran parlaklığını, zil seslerini, ahizeden, kulaklıktan ya da hoperlörden duyulan ses düzeyini kendileri ayarlayabilmelidir.
      13. Telefon, DHCP sunucudan IP adresini kendisi alabilmeli ya da statik IP adresi ile konfigüre edilebilmelidir. Telefon, otomatik olarak çağrı yöneticisine kayıt olabilecek ve TFTP sunucudan konfigürasyon bilgilerini alabilecektir. TFTP ile firmware güncellemesi yapılabilecektir.
      14. Uzak noktalardaki telefonlar, merkez noktadaki çağrı yöneticisi ile çalışabilmelidir. Telefonlar, WAN hatlarındaki bir kopukluk durumunda yedekli çalışmayı desteklemelidirler.
      15. Telefon, XML (Extensible Markup Language) uygulamalarını desteklemelidir.
      16. Telefon masa üstünde durabileceği gibi, duvara da monte edilebilmelidir.
      17. Ekran üzerinde cevapsız çağrılar, arayan isim ve numara, arama süresi, tarih ve zaman bilgileri gösterilecektir.
      18. SIP tabanlı haberleşmeyi desteklemelidir.
      19. Telefon üzerinde sabit çağrı bekletme, transfer ve konferans tuşu bulunmalıdır.
      20. Telefon üzerinden tek bir tuş yardımı ile kurumsal rehbere ve sesli mesaj servisine erişim mümkün olabilmelidir.
      21. Telefon, çağrı bekletme (call hold), çağrı aktarma (call transfer), çağrı yönlendirme (call forward), aynı hattan ikinci çağrıyı alabilme (call waiting), üçlü ya da daha çok kişiyle görüşme (conference), tek tuşla arama (speed dial), çağrı parketme (call park), çağrı çekme (call pick-up) özelliklerini desteklemelidir.
      22. Telefon ile çağrı yöneticisi arasında, sayısal sertifikalar aracılığı ile kimlik doğrulaması ve şifreli haberleşme yapılabilmelidir.
      23. Telefon ile diğer güvenli haberleşmeyi destekleyen telefonlar arasında şifreli görüşmeler (authenticated and encrypted calls) yapılabilmelidir.
      24. Telefonun arayüzü Türkçe olmalıdır.
   10. **KABLOSUZ AĞ MASA TELEFONU TİP -3 (10 ADET)**
       1. Telefon, IEEE 802.11a/b/g/n/ac protokolünü desteklemeli ve kablosuz olarak IP haberleşmesi yapabilmelidir.
       2. Telefon 802.11r roaming protokolünü desteklemelidir.
       3. Bir telefona 6 adede kadar dahili hat verilebilmelidir.
       4. Telefon, G.711a, G.711u, G.729a, G.729ab, G.722, ve iLBC ses sıkıştırma algoritmalarını desteklemelidir. LAN ve WAN çağrılarında farklı codec kullanılabilmelidir.
       5. Telefonun 2.4-inc 240 x 320 pixel çözünürlüklü renkli ekranı olmalıdır.
       6. Telefonun kulaklık (headset) girişi olmalıdır.
       7. Bluetooth 3.0 kulaklık desteği olmalıdır.
       8. Kullanıcılar, telefonu kulak hizasına yaklaştırmak zorunda kalmadan karşı tarafla konuşabilmelidir (hands-free özelliği olmalıdır).
       9. Telefonun mikrofonu sessiz (mute) moduna alınabilmelidir.
       10. Telefon, DHCP sunucudan IP adresini kendisi alabilmeli ya da statik IP adresi ile konfigüre edilebilmelidir. Telefon, otomatik olarak çağrı yöneticisine kayıt olabilecek ve TFTP sunucudan konfigürasyon bilgilerini alabilecektir. TFTP ile firmware güncellemesi yapılabilecektir.
       11. Uzak noktalardaki telefonlar, merkez noktadaki çağrı yöneticisi ile çalışabilmelidir. Telefonlar, WAN hatlarındaki bir kopukluk durumunda yedekli çalışmayı desteklemelidirler.
       12. Telefon, XML (Extensible Markup Language) uygulamalarını desteklemelidir.
       13. Telefonun standart pili 9.5 saat konuşma ve 145 saat stand-by süresine sahip olan Lityum-iyon pil olmalıdır.
       14. Çalışma sıcaklığı -10ºC / +50ºC, saklama sıcaklığı -30ºC / +60ºC arasında olmalıdır.
       15. Telefon, çağrı bekletme (call hold), çağrı aktarma (call transfer), çağrı yönlendirme (call forward), aynı hattan ikinci çağrıyı alabilme (call waiting), üçlü ya da daha çok kişiyle görüşme (conference), tek tuşla arama (speed dial), çağrı parketme (call park), çağrı çekme (call pick-up) özelliklerini desteklemelidir.
       16. Telefon 40 ve 128 bit uzunluğundaki statik WEP şifrelerini, WPA ve WPAv2 dinamik şifreleme protokolünü desteklemelidir.
       17. Telefon ile çağrı yöneticisi arasında, sayısal sertifikalar aracılığı ile kimlik doğrulaması ve şifreli haberleşme yapılabilmelidir.
       18. Telefon ile diğer güvenli haberleşmeyi destekleyen telefonlar arasında şifreli görüşmeler (authenticated and encrypted calls) AES-128 şifreleme yöntemi kullanılarak yapılabilmelidir.
       19. EAP/TLS, SHA-1 ve SHA-2 gelişmiş şifreleme imzaları ve otomatik olarak, telefonlardaki sertifikaların yenilenebilmesini sağlayan SCEP (Simple Certificate Enrolment Protocol) protokollerini desteklemelidir.
       20. IP67 ve MIL-STD-810G yüksek seviye koruma ve güvenlik standartlarını desteklemelidir.
   11. **ÇAĞRI KONTROL SİSTEMİ**
       1. Ürün sinyalleşme ve medya şifreleme işlemlerinde TLS ve SIP SRTP kullanabilmelidir. Bu işlemler için minimum AES 256 kriptolama desteğine sahip olacaktır.
       2. Çağrı kontrol sisteminde En az SHA-512 ve RSA 3072 bit anahtarlar desteklenmelidir.
       3. H.265 video codec desteğine sahip olmalıdır
       4. Sistem üzerindeki bütün cihazlar ve uygulamalar birbirleri ile IP tabanlı olarak haberleşmelidir. Telekom bağlantısı ve analog cihaz bağlantıları haricinde sistemin hiçbir parçası TDM tabanlı olarak çalışmayacaktır.
       5. Sistem üzerinde uç çihaz olarak IP telefon, yazılım tabanlı telefon, masaüstü görüntülü telefon, masaüstü görüntülü konferans, oda tipi görüntülü konferans ve mobil telefonlar üzerinde çalışan uygulamaları kullanılabilmelidir. Bu ürünler sistem üreticisinin ürünü olmalıdır.
       6. Sistemin yazılım yedeği istendiği an ya da önceden belirlenmiş zaman aralıklarında otomatik olarak alınabilmelidir.
       7. Ürün ile aynı marka Video Konferans cihazlarının ve IP Telefon setlerinin kullanıcı ara yüzünün Türkçe desteği olmalıdır.
       8. IP Çağrı Kontrol Sistemi kurumun sağlayacağı Vmware tabanlı sanal kaynaklarda yedekli olarak kurulacaktır.
       9. IP Çağrı Kontrol Sistemi yedekli donanıma sahip olacak şekilde teklif edilmelidir. Çağrı kontrol sistemi; üretici menşeili en az 1 adet sunucu üzerinde çalışacaktır. IP Çağrı Kontrol Sistemi’nde aktif çağrı yöneticisinin devre dışı kalması durumunda, aktif görüşmeler kesinti olmadan devam edecektir.
       10. Sunucu üzerinde en az 2.2 GHz hızında en az 10 çekirdekli 1 adet işlemci bulunacaktır.
       11. Her bir sunucuda en az 48 GB RAM bulunacaktır.
       12. Her bir sunucu en az 6 adet 300 GB 10K RPM disk ile teklif edilecektir. Diskler hot-swappable olacaktır.
       13. Teklif edilecek sunucu, çağrı kontrol sistemi ile aynı üreticiye ait olmalıdır.
       14. Teklif edilecek Çağrı Kontrol Sistemi IP tabanlı olacaktır.
       15. IP servis kalitesi parametreleri – QoS (802.1p/Q, RSVP, Call Admision Control - Data hattı dolu iken çağrının farklı şekilde, örneğin PSTN üzerinden yönlendirilmesini sağlayan sistem) bulunmalıdır.
       16. Teklif edilen sistem, maksimum kapasitesine artırılmak istendiğinde yapılmış olan yatırım âtıl duruma düşürülmeden kapasite yükseltilmesi yapılabilmelidir.
       17. Çağrı kontrol sistemi 720p ve 1080p çözünürlükte video sinyalleşmesini desteklemelidir. Kendi başına destekleyemiyorsa eş zamanlı 500 adet FullHd kalitede görüşme yapılabilmesini destekleyen bir ürün çözüme dahil edilmelidir.
       18. Tüm sistem ve cihaz konfigürasyonları ile arama planları veri tabanında saklanacaktır.
       19. H.323 ve SIP trunking protokollerini desteklemelidir
       20. Çağrı Kontrol Sistemi ilave donanım gerektirmeden SIP protokolünü destekleyen IP Telefonları desteklemelidir.
       21. Kullanıcılar telefonlarının çalma seslerini seçebilmeli ve ses yüksekliğini ayarlayabilmelidirler.
       22. İç ve dış aramalarda arayan numara bilgisi ekranlı telefon setleri üzerinde gözükebilmelidir.
       23. Telefon setleri çağrı yöneticisine otomatik olarak kayıt olup çalışmaya başlayabilmelidir. İstenmesi durumunda bu özellik kapatılabilmelidir.
       24. Kullanıcının meşgul olması durumunda gelen aramalar istenilen bir numaraya yönlendirebilmelidir.
       25. Telefonlar üzerinde aranan numara bilgisi gözükmelidir.
       26. Telefonlar üzerinde cevapsız çağrı numaraları, aranan numaralar ve arayan numaralar liste olarak gözükmelidir.
       27. Tek numaradan erişim (single number reach) özelliği desteklenmelidir.
       28. Sistemde çalışan bir rehber uygulaması bulunmalı ve bu sayede kullanıcılar aradıkları kişinin ismini aratarak numarasını bulmalı ve doğrudan telefon üzerinden arayabilmelidir.
       29. Kullanıcılar kendi adres defterlerini oluşturabilmelidir.
       30. Rehber servisleri için Active Directory veya LDAP Directory sistemleri kullanılabilmelidir.
       31. Kullanıcı adı ve şifreye bağımlı farklı yetki seviyelerinde sistem yöneticileri tanımlanabilecektir.
       32. Çağrı yöneticisi arayüzünde H.323,SIP ve MGCP ses geçitleri tanımlanabilmelidir.
       33. Çağrı Kontrol Sistemi üreticisinin aynı marka kulaklık çözümü de olmalı ve bu kulaklıklarla ilgili ses seviyesi, mikrofon kazancı ve bas/tiz ayarları Çağrı Kontrol Sistemi web arayüzünden yapılabilmelidir.
       34. Çağrı Kontrol Sistemi web arayüzünden son 30 gün içinde aktif veya inaktif durumda olan aynı veya farklı marka kulaklık modelleri envanter olarak görüntülenebilmelidir.
       35. Çağrı Kontrol Sistemi web arayüzünden Çağrı Kontrol Sistemi ile aynı marka kulaklıklar için seri numara,eşleştiği son kullanıcı bilgisi,kullandığı yazılım versiyonu ve bağlı olup olmadığı bilgisi görümntülenebilmelidir.
       36. Çağrı Kontrol Sistemi TLS(Transport Layer Security) 1.2 versiyonunu destekleyecektir.
       37. Güvenlik kriterlerinin üst düzeyde sağlanması için ; Çağrı Kontrol Sistemi ile kurulacak olan güvenli bağlantılarda TLS versiyonunun minimum 1.2 olması opsiyonel olarak seçilebilecek ve TLS 1.2 versiyonundan daha önceki TLS versiyonlarının bağlantı kurması engellenebilecektir.
       38. Çağrı Kontrol Sistemi yöneticisine başvurmaya gerek kalmadan, arızalı bir IP tabanlı masa telefonunu kullanıcılar Self-Provisioning IVR hizmetini kullanarak değiştirebilmelidir.
       39. Çağrı Kontrol Ünitesi Gelişmiş güvenlik modunda çalışabilmelidir.Bu modda iken aşağıdaki özellikler desteklenecektir.
       40. Kullanıcı şifreleri ve şifre değişiklikleri için katı politika ilkeleri uygulanacaktır.
       41. Şifre uzunluğu minimum 14 karakterden oluşacaktır.
       42. Şifre için minimum 1 adet küçük harf,1 adet büyük harf,1 adet rakam ve 1 adet özel karakter kullanılması zorunlu olacaktır.
       43. Geçmişe dönük son kullanılan 24 şifreden farklı bir şifre olacaktır.
       44. Eski şifreye göre yeni tanımlanan şifrenin en az 4 adet karakteri bir önceki şifreden farklı olması zorunlu olacaktır.
       45. Uzaktan denetim günlüğü yapılandırılabilmeli ve yapılandırılırsa, TCP uzak günlükler için varsayılan aktarım protokolü olacaktır.
       46. Çağrı Kontrol Sistemi 110 adet kullanıcı lisansı ile teklif edilecektir. Lisanslar 3 yıllık süreyle kullanılabilecek ve bu süre içerisinde minor ve major güncellemeler için gerekli dosyalara erişim imkânı sağlanacaktır.
       47. İşbu şartname de temin edilecek donanım ve yazılımları için doğrudan kurum adına üretici firma teknik merkezine Web üzerinden veya telefon ile problem bildirme, destek alma, ürünlerin yazılım güncellemeleri ve arızalı ürünlerin yenisiyle değiştirilmesi hizmeti sağlanacaktır. Yüklenici, teklifinde bu üretici servis hizmetlerini teklif ettiğine dair Yetki Belgesini üretici firmadan veya yetkili distributer’ünden temin ederek ihale dosyasında kuruma sunacaktır. Bu hizmet 3 yıl için en az aşağıdaki servis olanaklarını karşılayacaktır;
       48. Üretici Firmanın Teknik Yardım Merkezi’ne 7x24 erişim imkânı
       49. Ücretsiz İşletim Sistemi güncellemeleri ve yükseltmeleri
       50. Donanımlar için 5x8, hafta içi çalışma saatlerine bağlı olarak ertesi iş günü içinde parça tedariği
       51. Bakım hizmeti alınan ürünlerinin kurum adına üretici firma teknik destek servisine kaydettirildiğine dair yazılı belge, sözleşme öncesinde kabule esas doküman olarak, üretici firmadan veya yetkili distribütör ’ünden alınıp kuruma teslim edilecektir.
   12. **SES GEÇİT ROUTER (1 ADET)**
       1. Şasi tipli, genişlemeye açık ve modüler bir yapıya sahip olmalıdır.
       2. Cihaz üzerinde fiziksel olarak, en az 2 adet 10/100/1000 Mbps bakır RJ-45 Gigabit Ethernet ve en az 1 adet 1000BaseX SFP portu bulunmalıdır. Aynı anda 2 port aktif olarak çalışabilmelidir.
       3. Cihaz üzerinde, 2 adet geniş alan ve ses modüllerinin takılabileceği WAN slotu, 1 adet Service Module slotu ve en az 1 adet PVDM (Packet Voice Digital Signal Processor Module) slotu, bulunmalıdır.
       4. Cihaz üzerinde en az 30 oturum açılacak SIP lisansı teklife dahil edilmelidir.
       5. En az 4 GB MB DRAM’i olmalıdır. DRAM, 16 GB’e kadar arttırılabilmelidir.
       6. Cihaz üzerinde en az 4 GB Flash bulunmalıdır. İstenmesi durumunda ilave donanım ile 16 GB’e kadar arttırılabilmelidir.
       7. Cihazın aggregate throughput değeri en az 50 Mbps olmalıdır. Sadece lisans arttırımı ile bu değer 100 Mbps’ e kadar çıkabilmelidir.
       8. Cihaz üzerinde, gerekli ayarlamaların yapılabilmesi için, aynı anda 1 tanesi kullanılmak üzere, 1 adet standart RJ-45 ve 1 adet USB konsol portu olmalıdır.
       9. Şebeke arabirim kartları ihtiyaca göre sistem üzerindeki slotlara takılabilmelidir. Çeşitli arabirimlerde Fast Ethernet, Gigabit Ethernet, 3G/4G kartı, ADSL/VDSL, kanallı E1 portları cihaz tarafından desteklenebilmelidir.
       10. Cihaz üzerinde yazılım temelli güvenlik duvarı özelliği gerekli yazılım ve lisans artırımları ile sağlanabilir olmalıdır.
       11. İstenmesi durumunda gerekli lisans artırımı ile uzak alan ağ optimizasyonu özelliği (Wide Area Acceleration Services) desteklenebilmelidir.
       12. Cihaz, FXS, FXO ve E&M gibi analog ses ve E1 gibi sayısal ses portlarını destekleyen arabirim kartlarını desteklemelidir.
       13. Yönlendirici üzerinde IP adres ve TCP/UDP port bazında kısıtlama sağlayacak erişim denetim listeleri tanımlanabilmelidir.
       14. RADIUS, TACACS, AAA gibi güvenlik protokollerini desteklemelidir.
       15. Bandwidth on demand, dial backup, dial on demand özelliklerini ve RIP, RIPv2, OSPF, BGP gibi yönlendirme protokollerini desteklemelidir.
       16. Cihaz üzerinde, statik, RIP, OSPF, BGP protokollerinin IPv6 versiyonu yönlendirme protokolleri desteklenmelidir.
       17. Cihaz üzerinde, multicast desteği olmalıdır. PIM (Protocol Independent Multicast) SM, SSM ( Source Specific Multicast ) destekleri sağlanabilmelidir.
       18. Cihaz üzerinde MPLS (Multi Protocol Label Switching) desteği lisans arttırımı ile sağlanabilir olmalıdır.
       19. Trafik önceliklendirmesi yapılabilmeli ve WAN bağlantısı üzerinde belirli uygulamalara (VoIP, http, smtp vs.) özel bant genişliği açılabilmelidir.
       20. Konfigürasyonu grafik ortamlarda çalışabilen bir programla yapılabilmelidir
       21. Yönetim amaçlı SNMP, RMON, dahili WEB server ve TELNET protokollerini desteklemelidir.
       22. Üzerindeki yazılım istenen özellikleri destekleyecek nitelikte ve güncel olmalıdır.
       23. Teklif edilen ürün, ömür boyu üretici garantisine sahip olacaktır ve bununla birlikte üretici tarafından sağlanan en az 3 yıllık 8x5xNBD (çalışma saatleri ve çalışma günleri içerisinde ertesi gün değişim) servis paketi ile teklif edilecektir.
   13. **GARANTİ ve DİĞER HUSUSLAR**
       1. Şartnamede belirtilen gereksinimler içerisinden karşılanamayan ya da kısmi/koşullu olarak karşılanabilen maddeler var ise açıklamaları ile birlikte madde bazında teklife eklenmelidir. Aksi takdirde ilgili maddelerin verilen teklif kapsamında kabul edildiği varsayılacaktır. Aynı zamanda belirtilen gereksinimlerin üzerine ek olarak sağlanan çözümler de teklif içerisinde belirtilmelidir.
       2. Cihaz modellerinin üretimden kalkması durumunda, verilecek siparişlerde Yüklenici tarafından teknik şartnameyi karşılayacak özellikte eşdeğer veya bir üst modelde ürün verilecektir.
       3. Satın alınacak olan tüm cihazlar CE belgesine ve bu belge ile birlikte FCC veya TUV belgelerinden en az birine sahip olacaktır. Bu belgeler teklif dosyasına eklenecektir.
       4. Donanım, sipariş edildiği ülke veya bölgenin yerel enerji ve bağlantı standartlarına uygun şartlarda olacaktır.
       5. Şartnamede tarif edilen ürünlerin tamamını sağlayan Yüklenici’nin teklifleri öncelikli tercih edilecektir.
       6. Verilen siparişlerin teslim süresi 10-12 hafta olacaktır. Pandemi koşulları sebebiyle olacak gecikmeler üreticiden alınacak resmi bir yazı ile bildirilmek durumundadır.
       7. Satın alınacak teklif tablosunda yer alan tüm cihazlar tüm aksesuar/aparatlarıyla parça, özellik ve işçilik dahil en az 3 yıl üretici garantili olacaktır.
       8. Yüklenici, teklif ettiği ürün için Yetkili Servis Merkezi ve Çözüm Ortağı olduğunu belgelemelidir.
       9. Yüklenici, Teklif ettiği ürün için en üst düzey Partner derecesine sahip olmalıdır.
2. **MASAÜSTÜ BİLGİSAYAR**
   1. **MASAÜSTÜ BİLGİSAYAR - AIO TEKNİK GEREKSİNİMLERİ (120 Adet)**
      1. Teklif edilecek ürün en az 10. Nesil ve Intel Core i7-10700 Processor vPro (16MB Cache, up to 4.70GHz with Turbo Boost) işlemciye sahip olmalıdır.
      2. Teklif edilecek ürün en az 16GB DDR4 2933Mhz belleğe sahip olmalıdır. Ürün 64GB belleğe kadar yükseltilebilir olmalıdır. En az 2 bellek yuvasına sahip olmalı ve en az bir bellek yuvası boş olmalıdır.
      3. Teklif edilecek ürün en az 512GB kapasiteli SSD, PCIe-NVMe ve Opal özellikli sabit disk’e sahip olmalıdır.
      4. Teklif edilecek üründe dahili olarak Intel UHD Graphics 630 ekran kartı bulunmalıdır.
      5. Teklif edilecek ürün kurumsal segmentteki Intel Q470 veya daha üst düzey yonga setine sahip olmalıdır.
      6. Teklif edilecek ürün ekranı tümleşik dokunmatik olmayan 23.8” (1920x1080) çözünürlükte 16,9 ve IPS özelliğine sahip olmalıdır.
      7. Teklif edilecek ürün ekranı Kontrast Değeri en az 1000:1, Parlaklık en az 250 nits, Anti Glare özelliğinde olacaktır.
      8. Teklif edilecek ürün yarım yükte %85 verimlilikte en az 170W’lık güç adaptörüne sahip olacaktır.
      9. Teklif edilecek ürün ile birlikte kablolu USB Türkçe Klavye ve USB Optik Mouse verilmelidir. Verilecek donanımlar sistem ünitesi ile aynı marka olmalıdır.
      10. Teklif edilecek üründe hoparlör PC ile bütünleşik olmalı 2x3W gücünde olmalıdır. Mikrofon ve Kulaklık combo çıkışı bulunmalıdır.
      11. Teklif edilecek üründe en az 1080P Webcamera bulunmalıdır.
      12. Teklif edilecek üründe 10/100/1000 Ethernet portuna sahip olmalıdır. (RJ45).
      13. Teklif edilecek üründe Dual Band, çift antenli AC destekli kablosuz ağ bulunmalıdır. (Intel Wireless-AC 9560 2x2 AC)
      14. Teklif edilecek ürün Windows 10 Pro 64 bit yüklü olarak verilmelidir. Ön kurulum ekranında Türkçe ve İngilizce Dil seçeneğini sormalıdır.
      15. Teklif edilecek ürün en fazla stand hariç 545 X 48 X 350 (mm) ölçülerinde ve 5,30kg ağırlığında olmalıdır. Stand dahil edildiğinde 545 X 210 X 415 to 500(mm) ölçülerini ve 7,55kg ağırlığını geçmemelidir.
      16. Teklif edilecek ürün Wake-on-LAN özelliğini desteklemelidir.
      17. Teklif edilecek ürün TPM 2.0 (Trusted Platform Module), Secure Boot, UEFI ve Virtualization Technology (Vt-x), Virtualization Technology for Directed I/O (VT-d) ve Credential Guard ve Device Guard özelliklerine sahip olacaktır.
      18. Teklif edilen üründe arka tarafta en az 4 adet USB 3.2 Gen1 , Yan tarafta en az 2 adet USB 3.2 Gen2, 1 adet USB-C 3.2 Gen1 port bulunmalıdır.
      19. Teklif edilecek üründe en az 1 adet DP(Display Port) bulunmalıdır.
      20. Teklif edilecek ürün Energy Star belgeli olmalıdır.
      21. Teklif edilecek ürün 3 Yıl Yerinde servis garantisine sahip olmalıdır.
   2. **MASAÜSTÜ MİNİ BİLGİSAYAR - (17 Adet)**
      1. Teklif edilecek ürün en az 10. Nesil ve Intel Core i7-10700T Processor(16MB Cache, up to 4.40GHz with Turbo Boost) işlemciye sahip olmalıdır.
      2. Teklif edilecek ürün en az 16GB DDR4 2933Mhz belleğe sahip olmalıdır. Ürün 64GB belleğe kadar yükseltilebilir olmalıdır. En az 2 bellek yuvasına sahip olmalı ve en az bir bellek yuvası boş olmalıdır.
      3. Teklif edilecek ürün en az 512GB kapasiteli SSD, PCIe-NVMe ve Opal özellikli sabit disk’e sahip olmalıdır.
      4. Teklif edilecek üründe dahili olarak Intel UHD Graphics 630 ekran kartı bulunmalıdır.
      5. Teklif edilecek ürün kurumsal segmentteki Intel H470 veya daha üst düzey yonga setine sahip olmalıdır.
      6. Teklif edilecek ürün yarım yükte %85 verimlilikte en az 135W’lık güç adaptörüne sahip olacaktır.
      7. Teklif edilecek ürün ile birlikte kablosuz USB Türkçe Klavye ve kablosuz USB Optik Mouse verilmelidir. Verilecek donanımlar sistem ünitesi ile aynı marka olmalıdır.
      8. Teklif edilecek üründe hoparlör PC ile bütünleşik olmalı 1x1,5W gücünde olmalıdır. Mikrofon ve Kulaklık combo çıkışı bulunmalıdır.
      9. Teklif edilecek üründe VESA bağlantı aparatı bulunmalıdır. (Ürünler ile birlikte asansör ayaklı monitörler için kullanılacak ek kitler ürünle birlikte verilmelidir.)
      10. Teklif edilecek üründe 10/100/1000 Ethernet portuna sahip olmalıdır. (RJ45).
      11. Teklif edilecek üründe Dual Band, çift antenli AX destekli kablosuz ağ bulunmalıdır. (Intel Wi-Fi 6 AX201 2x2 AX).
      12. Teklif edilecek ürün Windows 10 Pro 64 bit yüklü olarak verilmelidir. Ön kurulum ekranında Türkçe ve İngilizce Dil seçeneğini sormalıdır.
      13. Teklif edilecek ürün en fazla 180 x 185 x 37 (mm) ölçülerinde ve 1,30kg ağırlığında olmalıdır. (Vesa bağlantı aparatı bu değerlere katılmamıştır.)
      14. Teklif edilecek ürün Wake-on-LAN özelliğini desteklemelidir.
      15. Teklif edilecek ürün TPM 2.0 (Trusted Platform Module), Secure Boot, UEFI ve Virtualization Technology (Vt-x), Virtualization Technology for Directed I/O (VT-d) ve Credential Guard ve Device Guard özelliklerine sahip olacaktır.
      16. Teklif edilen üründe Arka tarafta en az 4 adet USB 3.2 Gen1, 1 Adet Ethernet (RJ45), 1 Adet HDMI, 1 Adet Display Port, Ön tarafta en az 1 adet USB 3.2 Gen2, 1 adet USB-C 3.2 Gen1 ve kulaklık/mikrofon combo port bulunmalıdır.
      17. Teklif edilecek ürün Energy Star belgeli olmalıdır.
      18. Teklif edilecek ürün 3 Yıl Yerinde servis garantisine sahip olmalıdır.
   3. **GARANTİ ve DİĞER HUSUSLAR**
      1. Şartnamede belirtilen gereksinimler içerisinden karşılanamayan ya da kısmi/koşullu olarak karşılanabilen maddeler var ise açıklamaları ile birlikte madde bazında teklife eklenmelidir. Aksi takdirde ilgili maddelerin verilen teklif kapsamında kabul edildiği varsayılacaktır. Aynı zamanda belirtilen gereksinimlerin üzerine ek olarak sağlanan çözümler de teklif içerisinde belirtilmelidir.
      2. Cihaz modellerinin üretimden kalkması durumunda, verilecek siparişlerde Yüklenici tarafından teknik şartnameyi karşılayacak özellikte eşdeğer veya bir üst modelde ürün verilecektir.
      3. Satın alınacak olan tüm cihazlar CE belgesine ve bu belge ile birlikte FCC veya TUV belgelerinden en az birine sahip olacaktır. Bu belgeler teklif dosyasına eklenecektir.
      4. Donanım, sipariş edildiği ülke veya bölgenin yerel enerji ve bağlantı standartlarına uygun şartlarda olacaktır.
      5. Şartnamede tarif edilen ürünlerin tamamını sağlayan Yüklenici’nin teklifleri öncelikli tercih edilecektir.
      6. Verilen siparişlerin teslim süresi 10-12 hafta olacaktır. Pandemi koşulları sebebiyle olacak gecikmeler üreticiden alınacak resmi bir yazı ile bildirilmek durumundadır.
      7. Satın alınacak teklif tablosunda yer alan tüm cihazlar tüm aksesuar/aparatlarıyla parça, özellik ve işçilik dahil en az 3 yıl üretici garantili olacaktır.
      8. Yüklenici, teklif ettiği ürün için Yetkili Servis Merkezi ve Çözüm Ortağı olduğunu belgelemelidir.
      9. Yüklenici, Teklif ettiği ürün için en üst düzey Partner derecesine sahip olmalıdır.
3. **MICROSOFT LİSANSLARI TEKNİK ŞARTNEMESİ**
   1. **MICROSOFT LİSANSLARI KAPSAMI**
      1. Teklif edilecek olan Backup Sunucusu hariç diğer verilen Windows sunucu lisansları host bazında sınırsız sanal sunucu kurma hakkını barındırmalıdır.
      2. Temin edilecek Windows Sunucu lisansı Hibrit entegrasyon, korumalı sanal makineler, yazılımla tanımlanmış ağ ve yazılımla tanımlanmış depolama özelliğini içermelidir.
      3. Teklif edilecek lisansların Yazılım Güvencesi (Software Assurance) içermesi gerekmektedir.
      4. Teklif edilecek olan lisanslar kiralama modeli ile temin edilecektir.
      5. Yeni alım ve yenileme kapsamında temin edilecek tüm lisanslar belirtilen e-mail adresine tanımlanacaktır ve Volume Licensing Service Center üzerinden ürün anahtarları görüntülenebilir ve kurulum ISO’ları indirilebilir olmalıdır.
      6. Lisansları temin edecek kuruluşun Microsoft kiralama anlaşmaları kapsamında müşteri tarafından sahip olunun Planning Services voucher’ları için müşteriye Sharepoint Deployment Planning Services hizmeti sağlamak için gerekli yetkinliğe sahip olmalıdır.
      7. Lisansları temin edecek kuruluşun aşağıdaki partnerliklere minimumda sahip olması ve bu partnerlikleri Microsoft’un partnerler sitesi üzerinden ispatlayabilir olması tercih sebebidir.

    \*Gold Cloud Productivity

 \*Gold Application Development

\*Gold Datacenter

\*Gold Small and Midmarket Cloud Solutions

\*Gold Collaboration and Content

* + 1. Lisansları temin edecek kuruluşun yukarıda belirtilen yetkinlikleri yanı sıra kurumsal segmentte SAM (Software Asset Management) çalışması yapma yetkisinin olması tercih sebebidir.
  1. **YÜKLENİCİNİN PERSONEL YETKİNLİKLERİ KAPSAMI** 
     1. Microsoft lisanslarını temin edecek firmada 2 adet Microsoft lisanslama uzmanı ve 1 adet Microsoft iş geliştirme uzmanı olması tercih sebebidir.
     2. Microsoft lisanslarını temin edecek firmanın tüm Microsoft lisans danışmanlık hizmetlerini bünyesinde yer alan uzmanlar tarafından vermesi zorunludur.
     3. Microsoft lisanslarını temin edecek olan firmada minimum 8 adet CRM danışmanı olacaktır ve bu personellerin sektörde minimum 2 yıl saha tecrübesi olması tercih sebebidir.
     4. Microsoft lisanslarını temin edecek olan firmada minimum 7 adet .Net developer olacaktır ve bu personellerin sektörde minimum 2 yıl tecrübesi olması tercih sebebidir.
     5. Microsoft lisanslarını temin edecek olan firmada minimum 1 adet Uluslararası Yazılım Test Yeterlilik Kurumu tarafından sertifikalı çalışan bulunacaktır.

1. **DİĞER KONULAR**
   1. **TANIMLAR**
      1. Aşağıda, hizmet verilirken kullanılabilecek bazı tanımlamalar açıklanmıştır.

|  |  |
| --- | --- |
| **Tanım** | **Açıklama** |
| **Arıza Çağrısı – Acil** | Arızanın para, itibar kaybına sebep olduğu veya çok sayıda çalışanın kritik bir BT hizmetini almasını engellediği durumlarda açılan çağrılardır. Sistem çalışmaz halde, iş süreçleri durmuş durumdadır.  Bu tip arızaya uzaktan veya gerektiğinde yerinde müdahale edilir. |
| **Arıza Çağrısı – Normal** | Acil olarak nitelendirilmeyen her türlü arıza çağrısını ifade eder. Bu tip arızaya uzaktan veya gerektiğinde yerinde müdahale edilir. |

* 1. **PROJE ESNASINDAKİ SLA SEVİYELERİ VE DİĞER HİZMET PARAMETRELERİ** 
     1. Aşağıda, projenin teslimine kadar olan sürede uygulanacak SLA’ler belirtilmiştir.
     2. Yüklenici, aşağıdaki SLA’lere uygun bir arıza/destek sistemi ve sürecini Kurum’un hizmetine projenin başlangıcında sunmalıdır.
     3. Yüklenici, SLA ve proje yapısına uygun eskalasyon şemasını da yine teklif ile birlikte kuruma sunmalıdır.

|  |  |  |  |
| --- | --- | --- | --- |
| **Hizmet Tipi** | **Adet** | **Çağrı Kapsamı** | **Müdahale Süresi** |
| **Arıza Çağrısı – Acil** | Sınırsız | 5x8 | En fazla 4 saat |
| **Arıza Çağrısı – Normal** | Sınırsız | 5x8 | En fazla 8 saat |

* 1. **YEMEK - ULAŞIM**
     1. Danışmanlara öğle yemeği, Üsküdar Üniversitesi tarafından sağlanacaktır.
     2. Danışmanların ulaşım hizmeti Üsküdar Üniversitesi tarafından sağlanmayacaktır. Yüklenicinin bununla ilgili lojistik planlamayı yapması gerekmektedir.
  2. **TEKLİF PARA BİRİMİ**
     1. Hizmet için verilen teklifler Türk Lirası cinsinden verilmelidir.

1. **FİNANSAL BİLGİLER**

* 1. **ZAMAN TABLOSU**

### 

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

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

* 1. **FİRMA TARAFINDAN DOLDURULACAK TABLOLAR**
     1. Aşağıdaki tablolar, ayrı bir dokümanda doldurularak Üsküdar Üniversitesi ile paylaşılmalıdır. Teklif vermek isteyen firma, aşağıdaki tablodaki bilgilerin haricinde ek şartlarını ve koşullarını, aşağıdaki bilgileri içermesi kaydı ile ekler halinde belirtebilir.
     2. Üsküdar Üniversitesi, referans olarak gösterilen proje/firmaları ziyaret etmek isteyebilir. Teklif veren firma, Üsküdar Üniversitesinin istemesi durumunda bu firmalara ziyaret planlamakla yükümlüdür.
     3. Yüklenici, tüm alt projeler için (Sunucu, veri depolama, yedekleme, bulut, Network, sistem odası kurulumu, sistem danışmanlıkları) en az 1’er adet referans sağlamalıdır.

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

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

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

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