ÜSKÜDAR ÜNİVERSİTESİ

TIP FAKÜLTESİ GENEL BT ALTYAPI PROJE ŞARTNAMESİ

İÇİNDEKİLER

1. 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.

2. 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.

3. 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 vemodellerini 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

4. İhtiyaç

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

1. SUNUCU TEKNİK GEREKSİNİMLERİ

2 ADET RACK TİPİ SUNUCU ALIMI

SANALLAŞTIRMA YAZILIMI YEDEKLEME YAZILIMI NETWORK SANALLAŞTIRMA YAZILIMI

2. STORAGE TEKNİK GEREKSİNİMLERİ

15TBSSD_45TBSAS VERİ DEPOLAMA ÜNİTESİ

3. MASAÜSTÜ BİLGİSAYAR TEKNİK GEREKSİNİMLERİ

TEKNİK ÖZELLİKLER

GENEL HUSUSLAR

4. NETWORK TEKNİK GEREKSİNİMLERİ

OMURGA ANAHTAR CİHAZI

KENAR ANAHTAR CİHAZI

KABLOSUZ AĞ SİSTEMİ

KABLOSUZ ERİŞİM CİHAZI

AĞ ERİŞİM KONTROL SİSTEMİ

DNS KATMANI GÜVENLİK ÇÖZÜMÜ

5. GÜVENLİK TEKNİK GEREKSİNİMLERİ

AĞ GÜVENLİK CİHAZI

BİLGİ GÜVENLİĞİ VE OLAY YÖNETİM YAZILIMI

WEB UYGULAMA GÜVENLİK CİHAZI

YÜK DENGELEME CİHAZI

YETKİLİ HESAP ŞİFRE YÖNETİMİ VE OTURUM İZLEME YAZILIMI

1 SUNUCU TEKNİK GEREKSİNİMLERİ

1.1 2 adet rack tipi sunucu

1.1.1 Teklif edilecek sunucu 19” standart kabinlere monte edilebilmeli ve en fazla 2U yüksekliğinde olmalıdır.

1.1.2 Teklif edilecek sunucu üzerinde en az iki adet fiziksel işlemci yuvası bulunmalı ve sunucu üzerinde her biri 2.2GHz hızında 14 çekirdeğe sahip ve en az 19.25 MB L3 Cache belleğe sahip 2 adet işlemci bulunmalıdır.

1.1.3 Teklif edilecek sunucu RDIMM, LRDIMM bellek tipini desteklemelidir ve sunucu üzerinde en az 24 adet bellek yuvası bulunmalıdır. Sunucunu 3TB’a kadar toplam bellek desteği bulunmalıdır ve her biri en az 2666MT/s hızında, en az 4 adet 32GB RDIMM bellek modülü kullanılarak toplam 128GB bellek bulunmalıdır.

1.1.4 Teklif edilecek sunucu üzerinde en az 8 adet 2.5” disk yuvası bulunmalıdır.

1.1.5 Teklif edilecek sunucu üzerinde elektrik kesilmesine karşı pil korumalı korumalı üzerinde en az 2GB uçucu olmayan bellek bulunan RAID denetleyecisi bulunmalıdır. RAID kartı donanımsal olarak RAID 0/1/5/10/50/60 yapabilme yeteneğine sahip olmalıdır.

1.1.6 Sunucu üzerinde en az 2 adet her biri minimum 300GB kapasitede ve 10K dönme hızına sahip, sunucu çalışırken sökülüp takılabilecek (hot-plug) 2 adet disk birimi bulunmalıdır.

1.1.7 Sunucu üzerinde en az 4 port 1Gb Ethernet bağlantı noktası bulunmalıdır.

1.1.8 Sunucu üzerinde en az 2 port 10 Gbps SFP+ fiziksel bağlantı noktası bulunmalıdır. Bu bağlantı noktalarının 2 adet 10Gb SR SFP+ transceiver modülü bulunmalıdır.

1.1.9 Sunucu üzerinde her biri 1 adet 16 Gbps porta sahip, en az iki adet FC HBA bulunmalıdır.

1.1.10 Teklif edilecek sunucu üzerinde en az 5 adet PCIe slotu bulunmalıdır.

1.1.11 Teklif edilecek sunucu üzerinde 1 tane VGA portu, en az 2 adeti ön tarafta olmak üzere toplam 4 adet USB portu bulunmalıdır.

1.1.12 Teklif edilecek sunucu üzerinde embedded olarak en az 16mb belleğe sahip ve en az 1920*1200 çözünürlüğü destekleyen grafik kartı bulunmalıdır.

1.1.13 Teklif edilecek sunucu üzerinde çalışırken sökülüp takılabilen en az 2 adet 750W güç ünitesi bulunmalıdır. Güç ünitelerinin bağlantılarına uygun en az 1,5m uzunluğunda 2 adet güç kablosu teklife dahil edilmelidir.

1.1.14 Sunucu üzerinde 1 Gb hızında fiziksel bağlantı noktasına sahip uzaktan yönetim modülü bulunmalıdır. Sunucuyu uzaktan yönetebilmek için gerekli lisans eklenmelidir. Bağlantı esnasında herhangi bir süre kısıtlaması olmamalıdır.

1.1.15 Teklif edilecek sunucunun çalışma esnasında kabinden öne çekilerek müdahale edilmesini sağlayacak üzerine baskı olduğunda eğilmesini engelleyecek aksesuarlara sahip metal alaşımlı kayan ray sistemi ve kablo yönetim kolu bulunmalıdır.

1.1.16 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.

1.1.17 Sunucu 3 yıl boyunca üretici garantisine sahip olmalı, 7x24 4 saat içinde destek paketine sahip olmalıdır.

1.2 SANALLAŞTIRMA YAZILIMI (4 Adet)

1.2.1 Sanallaştırma yazılımı kurumun mevcutta kullandığı lisans olan VMWare VSphere Enterprise Plus olmalıdır.

1.2.2 Sanallaştırma yazılımı toplamda 4 CPU'yu destekleyecek şekilde lisanslanmalıdır.

1.2.3 Sanallaştırma yazılımı 1 yıl 5x9 olacak şekilde üretici garantisi altında olmalıdır.

1.2.4 Sanallaştırma yazılımını verecek yüklenicinin VMWare Premier Partner olması ve VMWare Master Services Competency- Data Center Virtualization yetkinliğine sahip olması gereklidir.

1.2.5 Sanallaştırma yazılımını verecek yüklenici de en az 2 (iki) adet VCAP DCV Design sertifikasına sahip personel çalışmalıdır.

1.3 YEDEKLEME YAZILIMI (4 Adet)

1.3.1 Yedekleme yazılımı kurumun mevcutta kullandığı lisans olan Veeam Enterprise Plus olmalıdır.

1.3.2 Yedekleme yazılımı toplamda 4 CPU'yu destekleyecek şekilde lisanslanmalıdır.

1.3.3 Yedekleme yazılımı 1 yıl 5x9 olacak şekilde üretici garantisi altında olmalıdır.

1.4 NETWORK SANALLAŞTIRMA YAZILIMI (20 Adet)

1.4.1 Network sanallaştırma yazılımı, kurumun yapısında bulunan toplamda 20CPU'yu lisanslayacak şekilde konumlandırılmalıdır.

1.4.2 Network sanallaştırma yazılımı kurumun ihtiyaçları doğrultusunda VMWare NSX Advanced Edition olmalıdır.

1.4.3 Network Sanallaştırma yazılımını verecek yüklenici de en az 2(iki) adet Network Virtualization VCP sertifikasına sahip personel çalışmalıdır.

2 STORAGE TEKNİK ŞARTNAMESİ

2.1 15TBSSD_45TBSAS VERİ DEPOLAMA ÜNİTESİ

2.1.1 Önerilecek olan harici veri depolama sistemi üreticisi en son yayınlanan General Purpose Disk Arrays detaylarını içeren Gartner raporunda Magic Quadrant'da liderler (Leaders) bölgesinde yer almalıdır.

2.1.2 Harici Depolama Birimi üzerinde en az 2 adet denetleme birimi bulunmalıdır. Denetleme birimleri birbirini yedekleme ve aktif-aktif çalışma özelliğine sahip olmalıdır.

2.1.3 Teklif edilen veri depolama ünitesinin her bir kontrol ünitesi üzerinde en az 8 çekirdekli işlemci olmalıdır.

2.1.4 Teklif edilecek veri depolama sistemi üzerinde bulunan disk denetleme birimlerinin her birinin üzerinde DRAM tipinde, en az 64 GB, toplam en az 128 GB ön bellek bulunmalıdır.

2.1.5 Teklif edilecek disk ünitesinde herhangi bir sorun çıkması durumunda sistem içerisindeki herhangi bir parçanın (en az disk, controller, güç kaynağı, fanlar) değiştirilmesi, sistem çalışırken herhangi bir sistem kapanması gerektirmeden yapılabilmelidir.

2.1.6 Denetleme birimleri, disk genişleme birimlerine en az 12Gbps SAS protokolünü kullanarak bağlanmalıdır. Toplam olarak en az 48 Gbps hızında bir bant genişliği sağlanmalıdır.

2.1.7 Harici depolama birimi, teklif edilen denetleme birimleri ile en az 222 adet diske kadar ölçeklendirilebilir özellikte olmalıdır.

2.1.8 Teklif edilen veri depolama ünitesi en az 2PB ham (raw) kapasite desteğine sahip olmalıdır.

2.1.9 Harici depolama birimi üzerinde net kapasite hesabı yapılırken, üretici firmanın teknolojisi gereği kullanması gereken sistem alanları var ise (vault, işletim sistemi vb.) bu alanlar net kapasite hesaplaması haricinde tutulacaktır.

2.1.10 Veri Depolama ünitesi RAID 0, 5, 6, RAID 10 seviyelerini desteklemelidir.

2.1.11 Veri Depolama ünitesi ile SAS, NL-SAS, SSD diskler kullanabilmelidir.

2.1.12 Veri depolama sistemi sunucu bağlantıları amaçlı iSCSI, FC, SAS, protokollerini desteklemelidir.

2.1.13 Sistem üzerinde yüksek performans ihtiyacı için en az 12Gbps hızında 800GB, 960GB, 1.6TB, 1.92TB, 3.84 TB, 7.68TB ve 15.36TB SSD seçenekleri ve 1.92TB, 3.84TB SSD SED (Self-Encrypted disk) seçenekleri mevcut olmalıdır.

2.1.14 Sistem üzerinde 10.000rpm hızında 900GB, 1.2TB, 1.8TB, 2.4TB SAS seçeneği, 1.8TB, 2.4TB SAS SED (Self-Encrypted disk) seçeneği, 15.000rpm hızında 600GB, 900GB SAS ve 600GB, 900GB SAS SED (Self-Encrypted disk) seçeneği mevcut olmalıdır.

2.1.15 Teklif edilen veri depolama ünitesi self-encrypting diskleri (SED) SSD formatında desteklemelidir.

2.1.16 Teklif edilen sistem üzerinde 1.92TB kapasiteli SSD diskler ile en az 15TB SSD alan, 2.4TB diskler ile en az 45 TB SAS alan bulunmalıdır.

2.1.17 Teklif edilen veri depolama ünitesi toplamda en az 8 adet olmak üzere 1G/10/25G ISCSI, 12G SAS, 16 & 32G FC bağlantılarını desteklemelidir. Desteklenen protokoller aynı anda kullanılabilmelidir.

2.1.18 Sistem üzerinde toplamda en az 4 (sekiz) adet 16Gbps hızında FC bağlantı portu bulunmalıdır. Tüm portlar 16Gbps modüller ile dolu olmalıdır.

2.1.19 Sistem thin provisioning özelliğine sahip olmalıdır. Lisans gerekiyor ise teklife dahil edilmelidir.

2.1.20 Teklif edilecek olan harici disk ünitesi içerisinde snapshot (anlık kopya) ve clone (full kopya) desteklenecektir. En az 8192 snapshot desteklenecektir. Bu özellik için gerekli lisanslar ihtiyaç halinde ileride satın alınabilecektir.

2.1.21 Sistem senkron ve asenkron "replikasyon" yapabilmelidir. Replikasyon lisansları ücretsiz sağlanamalıdır.

2.1.22 Sistem tanımlanan volume'ler (LUN) üzerinde IOPS ve bant genişliği tanımlamasına izin vermelidir.

2.1.23 Sistem VMware Stretched Metro Cluster vMSC standardı ile uyumlu olmalıdır. Teklif edilen ürün vmware'in uyumluluk listesinde yer almalıdır.

2.1.24 Teklif edilen veri depolama sistemi Microsoft Windows Server, Oracle Solaris, HP-UX, Oracle Linux, IBM AIX, Novell NetWare, SLES, Apple, HPTru64, VMware, Citrix XenServer, RedHat işletim sistemlerini desteklemelidir.

2.1.25 Sistem VMware VAAI, VASA ve vVOL standardı ile uyumlu olmalıdır.

2.1.26 Sistem web tabanlı (HTLM5) güvenli tek bir ara yüz üzerinden yönetilmelidir.

2.1.27 Anlık ve geriye dönük performans izlemek için gerekli yazılım sistem ile birlikte teklif edilmelidir.

2.1.28 Sistem anlık veya geçmişe yönelik "tier" veya RAID seviyesi bazında rapor verebilmeli, anlık ve geçmişe yönelik "volume" veya sunucu performansının raporlanabilmesine aynı ara yüz üzerinden olanak sağlamalıdır.

2.1.29 Üreticinin aynı model veya daha üstü bir modeli ile federasyon mantığında bir cluster yapısı oluşturabilmelidir. Federayon yapısı ile sistemler arası otomatik ya da manuel tiering (katmanladırma) yapılabilmelidir. Volume'ler kullanıma göre farklı sistemlerdeki daha düşük maliyetli ortamlara aktarılabilmelidir.Veri Depolama Sisteminin kurulumları belirtilen lokasyonlara yüklenici tarafından yapılacaktır.

2.1.30 Veri Depolama Sisteminin çalışması için gerekli tüm kablo ve aksesuar yüklenici tarafından temin edilecektir.

2.1.31 Teklif edilen veri depolama ünitesi üretici tarafından sağlanan 7/24 esasına göre 3 (üç) yıl 4 saat içerisinde yerinde müdahale garantiye sahip olacaktır.

2.1.32 Teklif edilen veri depolama ünitesinin kurulumu, üreticinin yetkili sistem mühendisi tarafından yapılacaktır.

3 MASAÜSTÜ BİLGİSAYAR TEKNİK GEREKSİNİMLERİ

3.1 Masaüstü Bilgisayar Teknik Özellikler (59 Adet)

3.1.1 Teklif edilecek ürün en az Intel Core i7-7700 Processor (8MB Cache, up to 4.20GHz) işlemciye sahip olmalıdır.

3.1.2 Teklif edilecek ürün en az 16GB DDR4 2400Mhz belleğe sahip olmalıdır. Ürün 64GB belleğe kadar yükseltilebilir olmalıdır. En az iki bellek yuvası boş olmalıdır.

3.1.3 Teklif edilecek ürün en az 256GB kapasiteli SSD ve Opal özellikli sabit disk'e sahip olmalıdır.

3.1.4 Teklif edilecek ürün kurumsal segmentteki Intel B250 veya daha üst düzey yonga setine sahip olmalıdır.

3.1.5 Teklif edilecek ürün yarım yükte %85 verimlilikte en az 180W'lık güç kaynağına sahip olacaktır. 2. Bir disk ünitesini sorunsuz çalıştıracaktır.

3.1.6 Teklif edilecek ürün ile birlikte USB Türkçe Klavye ve USB Optik Mouse verilmelidir. Verilecek donanımlar sistem ünitesi ile aynı marka olmalıdır.

3.1.7 Teklif edilecek üründe hoparlör kasa ile bütünleşik olmalıdır. (Microphone / Speaker Önde), Microphone /Speaker (Line In / Line Out)Arkada.

3.1.8 Teklif edilecek üründe 10/100/1000 Ethernet portuna sahip olmalıdır.

3.1.9 Teklif edilecek ürün FreeDOS olarak verilmelidir.

3.1.10 Teklif edilecek ürün en fazla 95mm yatay kasa yüksekliğine sahip olmalıdır.

3.1.11 Teklif edilecek ürün Wake-on-LAN ve PXE özelliğini desteklemelidir.

3.1.12 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.

3.1.13 Teklif edilen üründe ön tarafta en az 4 adet USB 3.0 ve arka tarafta 2 adet USB 3.0 port ile 2 adet USB 2.0 port bulunmalıdır.

3.1.14 Teklif edilecek üründe 1 adet PCI Express yuvası bulunmalıdır.

3.1.15 Teklif edilecek üründe VGA, DP(Display Port) ve HDMI port bulunmalıdır. Olmayan Port için dönüştürücü ile sağlanabilir. Dönüştürücü ile sağlana port en fazla 1 adet olabilir. Dönüştürücü ürün kutusu içinde verilmelidir.

3.1.16 Teklif edilecek ürün Energy Star belgeli olmalıdır.

3.1.17 Teklif edilecek ürün 3 Yıl Yerinde servis garantisine sahip olmalıdır.

3.2 Masaüstü Bilgisayar – Leboratuvar Teknik Özellikler (31 Adet)

3.2.1 Teklif edilecek ürün en az Intel Core i7-8700 Processor (12MB Cache, up to 4.60GHz) işlemciye sahip olmalıdır.

3.2.2 Teklif edilecek ürün en az 16GB DDR4 2666Mhz belleğe sahip olmalıdır. Ürün 64GB belleğe kadar yükseltilebilir olmalıdır. En az iki bellek yuvası boş olmalıdır.

3.2.3 Teklif edilecek ürün en az 256GB kapasiteli SSD ve Opal özellikli sabit disk'e sahip olmalıdır.

3.2.4 Teklif edilecek ürün kurumsal segmentteki Intel Q370 veya daha üst düzey yonga setine sahip olmalıdır.

3.2.5 Teklif edilecek ürün yarım yükte %92 verimlilikte en az 400W'lık güç kaynağına sahip olacaktır. 2. Bir disk ünitesini sorunsuz çalıştıracak ve Harici Ekran kartı olarak Gforce GTX 1060 Ekran kartını çalıştırabilecektir.

3.2.6 Teklif edilecek ürün ile birlikte USB Türkçe Klavye ve USB Optik Mouse verilmelidir. Verilecek donanımlar sistem ünitesi ile aynı marka olmalıdır.

3.2.7 Teklif edilecek üründe hoparlör kasa ile bütünleşik olmalıdır. (Microphone / Speaker Önde), Microphone /Speaker (Line In / Line Out)Arkada.

3.2.8 Teklif edilecek üründe 10/100/1000 Ethernet portuna sahip olmalıdır.

3.2.9 Teklif edilecek ürün FreeDOS olarak verilmelidir.

3.2.10 Teklif edilecek ürün en fazla 166x322x412 ölçülerinde olmalıdır.

3.2.11 Teklif edilecek ürün Wake-on-LAN ve PXE özelliğini desteklemelidir.

3.2.12 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.

3.2.13 Teklif edilen üründe ön tarafta en az 2 adet USB 3.1 Gen2, 2 Adet USB 3.1 Gen1, 1 Adet USB 3.1 Type-C ve arka tarafta 4 adet USB 3.1 port bulunmalıdır.

3.2.14 Teklif edilecek üründe 2 adet PCIe 3.0x16 ve 1 Adet PCIe 3.0x1 genişletme yuvası bulunmalıdır.

3.2.15 Teklif edilecek üründe VGA, DP(Display Port) ve HDMI port bulunmalıdır. Olmayan Port için dönüştürücü ile sağlanabilir. Dönüştürücü ile sağlana port en fazla 1 adet olabilir. Dönüştürücü ürün kutusu içinde verilmelidir.

3.2.16 Teklif edilecek ürün Energy Star belgeli olmalıdır.

3.2.17 Teklif edilecek ürün 3 Yıl Yerinde servis garantisine sahip olmalıdır.

3.3 23” Monitör (90 Adet)

3.3.1 Ekran Boyutu 23” ebatında olmalıdır.

3.3.2 Ekran IPS teknolojisine sahip LED panel olmalıdır.

3.3.3 Ekran Çözünürlüğü FullHD (1920x1080) - (16:9) değerlerine sahip olmalıdır.

3.3.4 Kontrast Değeri en az 1000:1, Parlaklık en az 250 nits Tepkime süresi 6ms olmalıdır.

3.3.5 Görüş açısı en az 170°(Yatay) 170° (Dikey) olmalıdır.

3.3.6 Ekran Tak ve Çalıştır uyumlu olmalıdır.

3.3.7 Ürün sistem ünitesi ile aynı renk ve marka’da olmalıdır.

3.3.8 Ekran’da Display Port, HDMI ve VGA Portlaru bulunmalıdır

3.3.9 Ekran kutusundan Sistem ünitesi ile uygun bağlantı kuracak 1,8m görüntü kablosu olmalıdır.

3.3.10 Yüksekliği ayarlanabilir ayak bulunmalıdır.

3.3.11 Teklif edilecek ürün en az 2 Yıl Garantiye sahip olmalıdır.

3.3.12 Teklif edilecek ürün Energy Star belgeli olmalıdır.

3.4 Genel Hususlar

3.4.1 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.

3.4.2 Cihaz modellerinin üretimden kalkması durumunda, verilecek siparişlerde Yüklenici tarafından teknik şartnameyi karşılayacak özellikte eşdeğer veya bir üst modelde ürün verilecektir.

3.4.3 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.

3.4.4 Donanım, sipariş edildiği ülke veya bölgenin yerel enerji ve bağlantı standartlarına uygun şartlarda olacaktır.

3.4.5 Şartnamede tarif edilen ürünlerin tamamını sağlayan Yüklenici'nin teklifleri öncelikli tercih edilecektir.

3.4.6 Verilen siparişlerin teslim süresi en geç 8 hafta olacak, stoktan ürün teslim edilmesi tercih sebebi olacaktır.

3.4.7 Satın alınacak teklif tablosunda yer alan tüm cihazlar tüm aksesuar/aparatlarıyla parça, özellik ve işçilik dahil en az 3 yıl üretici garantili olacaktır.

3.4.8 Yüklenici, teklif ettiği ürün için Yetkili Servis Merkezi ve Çözüm Ortağı olduğunu belgelemelidir.

3.4.9 Yüklenici, Teklif ettiği ürün için en üst düzey Partner derecesine sahip olmalıdır.

4 NETWORK TEKNİK GEREKSİNİMLERİ

4.1 OMURGA ANAHTAR CİHAZI (1 Adet)

4.1.1 Anahtar 1U yüksekliğinde olacaktır.

4.1.2 Anahtarlama kapasitesi en az 3,2 Tbps, yönlendirme performansı 2,5 Bpps olacaktır.

4.1.3 Cihaz üzerinde an az 48 adet aktif 1/10G SFP+ ve 6 QSFP yuvası bulunmalıdır.

4.1.4 İstenmesi durumu her bir QSFP port uygun kablo kullanılarak 4 ad 100GE porta dönüştürülebilmelidir.

4.1.5 Cihaz üzerinde en az 2 adet dahili güç kaynağı bulunmalıdır. Cihaz üzerindeki güç kaynakları, cihaz çalışırken sökülüp takılabilmelidir.

4.1.6 "1/10Gbps SFP+" portların tümünde "10G SFP Transceiver" lar ile ayrıca "Direct Attached Copper DAC - Twinax" kablo bağlantısı desteklenmelidir.

4.1.7 "1/10Gbps SFP+" portların tümünde "SX" veya "LX" tipi "1G SFP Transceiver"lar desteklenmelidir.

4.1.8 "1/10Gbps SFP+" portların tümünde "TX" tipi "1G SFP Transceiver"lar desteklenmelidir.

4.1.9 IEEE 802.3ad Link Aggregation, IEEE 802.1D MAC Bridging/STP, IEEE 802.1Q VLAN Tagging, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) protokolleri desteklenecektir.

4.1.10 IEEE 802.1Q VLAN ID'si işaretleme desteği ve port bazında VLAN tanımlanabilecektir.

4.1.11 "ISL Trunking" veya "ISL PortChannel" desteklenmelidir.

4.1.12 En az 4096 adet VLAN desteklemelidir ve port bazında VLAN tanımı yapılabilmelidir.

4.1.13 En az 9216byte büyüklüğünde yüksek boyutlu iletim birimi (Jumbo Frame) desteği bulunmalıdır.

4.1.14 Anahtarlama cihazı, 96000 adete kadar yönlendirme tablosusunu ve 8000adet multicast route destekleyecektir. Bu desteğin sağlanabilmesi için gerekli her türlü donanım teklif edilecektir.

4.1.15 Anahtarlama cihazı, multicast yönlendirme yapabilecek, PIMv2, PIM-SM, and PIM-SSM destekleyecektir.

4.1.16 İki adetten daha fazla farklı anahtarlayıcı arasında yapılan farklı kombinasyonlardaki bağlantıların tümünün, "Spanning Tree" kullanımına gerek olmadan, aktif/aktif çalışabileceği şekilde "Virtual Cluster Switching Fabric" veya "Multipath" teknolojisi desteklenmelidir. Bu bağlantı 64 adette kadar yapılabilebilmelidir.

4.1.17 Herhangi bir sunucudan gelen yedekli bağlantılar, yapı içerisindeki herhangi iki veya daha fazla farklı anahtarlayıcıda sonlanacak şekilde port gruplaması yapılabilmelidir.

4.1.18 Adres tablosunda en az 64000 adet MAC adresi desteği olmalıdır.

4.1.19 En az 1 adet RJ-45 seri konsol yönetim portu ve en az 1 adet Out-of-band ethernet yönetim portu bulunmalıdır.

4.1.20 Manuel veya dinamik olarak port grubu (“Etherchannel”, “Link Aggregation Group” vb.) tanımlanabilmeli ve bir port grubunda en az 16 adet portu desteklemelidir.

4.1.21 Servis Kalitesi 802.1p (QoS), SP (Strict Priority) ve WRR (Weighted Round-Robin) kuyruklama desteği bulunmalıdır.

4.1.22 Anahtarlama cihazı üzerinde, hız sınırlandırma (rate limiting), trafik şekillendirme (traffic shaping) ve bant genişliği tahsisi yapılabilecek, trafiğin atandığı kuyruklarda göreceli ve mutlak önceliklendirme yapılabilecektir.

4.1.23 Anahtarlama cihazının QoS desteği bulunacaktır. 3’üncü katman DSCP ve 2’nci katman CoS (IEEE 802.1p (sekiz yüz iki nokta bir P)) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilecek ve gerektiğinde öncelik değerlerini değiştirebilecektir.

4.1.24 Paketleri 2’nci katman başlığındaki MAC adresi, 3’üncü katman başlığındaki kaynak/hedef IP adresi 4’üncü katman başlığındaki TCP/UDP port numarası bilgilerine göre sınıflandırabilecektir. Anahtarlama cihazı üzerindeki her bir portun en az 8 (sekiz) adet öncelik kuyruğu bulunacaktır. Kuyruk boyutları dinamik olarak ayarlanabilecektir.

4.1.25 Anahtarlama cihazı Layer 2 özelliklerinden Link Aggregation Control Protocol (LACP), Unidirectional Link Detection UDLD (standard and aggressive), Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), spanning-tree guards, and Transparent VLAN Trunk Protocol (TVTP) desteklemelidir.

4.1.26 Anahtarlama cihazı RIPv2, L3/L4 ACL, OSPFv2, EIGRP, Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Unicast Reverse-Path Forwarding (uRPF) gibi L3 özelliklerini üstünde gelen yazılım ve donanım ile desteklemelidir, istenmesi durumunda yazılım ve donanım eklemesi ile BGP ve VRF de destekleyebilmelidir.

4.1.27 İstenmesi durumunda kaynak adresine göre yönlendirme (Policy Based Routing - PBR) destekleyebilmelidir.

4.1.28 “IEEE 802.1AB Link Layer Discovery Protocol –LLDP” protokol desteği bulunmalıdır.

4.1.29 “RADIUS” ve “TACACS” protokolleri ile kimlik tanımlama özelliklerini desteklemelidir.

4.1.30 “STP BPDU” ataklarına karşın “BPDU Guard” ile “BPDU Filter” veya “BPDU Drop” özelliği bulunmalıdır.

4.1.31 “STP Root” olarak seçilmiş anahtarı, ataklara ve yapılandırma hatalarına karşı korunmasına yarayan “Root Guard” özelliği bulunmalıdır.

4.1.32 “Layer 2” seviyesinde erişim kontrol listesi (“Access Control List - ACL”) konfigürasyonunu desteklemelidir. Teklif edilecek anahtar en az 4000 adet giriş, 1000 çıkış yönünde ACL yazabilecek donanım ve yazılım özelliklerini destekleyecektir.

4.1.33 Anahtarlama cihazının IEEE 802.1x desteği bulunacak ve 802.1x ile VLAN Assignment ve dinamik ACL özelliklerini destekleyecektir.

4.1.34 “SSHv2 Secure Shell” protokolü ile uzaktan güvenli şekilde yönetilebilir olmalıdır.

4.1.35 “SNMPv1” ve “SNMPv2” yönetim protokolleri desteklenmelidir.

4.1.36 Network trafiğini takip etmek için port aynalama (“Port Mirroring” / “Switched Port Analyzer”) özelliği bulunmalıdır. Birden fazla portun trafiği tek bir porttan takip edilebilecektir.

4.1.37 “FTP” ve “Secure Copy (SCP)” protokolü desteği bulunmalıdır.

4.1.38 Yazılım güncellemeleri “FTP” protokolü veya “USB” hafıza diski kullanılarak yapılabilecektir.

4.1.39 Cihaz tüm rack mount , kablo ve aparatlarıyla birlikte kullanıma hazır olarak teklif edilmelidir.

4.1.40 Anahtarlama cihazı üzerindeki fan modülü çıkarılabilir tipte ve fanları yedekli özellikte olacaktır.

4.1.41 Tüm sistem ve bağlı donanımlar, 220 (iki yüz yirmi) V. ve 50 (elli) Hz. şebeke gerilimi ile beslenecek ve güç kabloları Türkiye şartlarına uygun olacaktır.

4.1.42 Anahtarlama cihazı, 0 (sıfır) °C ile +40 (artı kırk) °C arasındaki sıcaklıklarda ve bağıl nemi %5 (yüzde on) ile %95 (yüzde seksen beş) arasında olan ortamlarda sorunsuz çalışacaktır.

4.1.43 Anahtar üzerinde en az 14 adet 10G SR SFP+ modül teklif edilmelidir. Cihaz ile birlikte teklif edilen tüm fiber optik modüller aynı üreticinin orjinal ürünleri olmalıdır. OEM parça teklif edilmeyecektir.

4.2 KENAR ANAHTAR CİHAZI (18 Adet)

4.2.1 Anahtar üzerinde en az 48 adet 10/100/1000BaseT ethernet portu ve en az 2 adet SFP+ tabanlı yuva bulunmalıdır. Bu yuvalara 10GBASE-LR, 10GBASE-SR, 10GBASE-LRM, 1000BASE-LX/LH, 1000BASE-SX, 1000BASE-BX ve 1000BASE-ZX fiber arayüzleri takılabilmelidir. Anahtar üzerinde en az 1 adet (10GBASE-SR) ile teklif edilmelidir.

4.2.2 Anahtarın tüm portları tıkanmasız ve line-rate çalışmalıdır.

4.2.3 Anahtarlama bant genişliği en az 216 Gbps olmalıdır.

4.2.4 Anahtarın 64-Byte'lık L3 paketlerinde en az L2 anahtarlama performans değeri en az 130 Mpps olmalıdır.

4.2.5 En az 16,000 adet unicast MAC adresi desteklenmelidir.

4.2.6 En az 512MB DRAM'e sahip olmalıdır.

4.2.7 En az 128MB Flash belleği olmalıdır.

4.2.8 Cihazın MTBF (mean time between failure) değeri 230.000 saatten daha az olmayacak ve açıkca belirtilecektir.

4.2.9 Tüm portlar üzerinde IEEE 802.1Q VLAN trunking protokolü desteklenmelidir. Cihazın desteklediği VLAN ID sayısı en az 4000, aktif VLAN sayısı en az 1000 olmalıdır. Port bazında VLAN tanımlanabilmelidir.

4.2.10 Cihaz üzerinde en az 8 adet 10/100/1000Base T port ayrı ayrı kanal altında toplanıp, tek port gibi çalışabilmelidir. En az 24 adet kanal (Port-Channel) tanımlanabilmelidir. IEEE 802.3ad standardı desteklenmelidir.

4.2.11 Bütün 10/100/1000BaseT portlar hem half-duplex hem de full-duplex çalışabilir olmalıdır. Port hızları otomatik olarak algılanabilmelidir. IEEE 802.3x standardı desteklenmelidir.

4.2.12 Cihazın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir. Paketleri, ayrıca L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre sınıflandırabilmelidir. Cihaz üzerindeki her portun en az 4 adet kuyruğu bulunmalıdır.

4.2.13 Anahtarın her 10/100/1000 bakır portunda auto-MDIX (automatic medium-dependent interface crossover) özelliği bulunmalıdır.

4.2.14 Anahtar üzerinde, her porta ait durum/duplex/hız bilgisi veren LED'ler bulunmalıdır.

4.2.15 IEEE 802.3, 802.3u, 802.3ab standartlarını desteklenmelidir.

4.2.16 Anahtar, gerektiğinde harici bir güç kaynağı takılarak, güç kaynağı yedeklemesine sahip olabilmelidir.

4.2.17 Anahtar, TDR (Time Domain Reflector) özelliğini destekleyecektir.

4.2.18 Anahtar, jumbo frame desteğine sahip olmalıdır. Desteklenen jumbo frame'lerin uzunluğu, en az 9216 byte olmalıdır.

4.2.19 Fiber kablolardaki arızalar nedeniyle oluşabilecek tek yönlü trafik problemlerini belirleyip ilgili portu kullanım dışı bırakarak, olası bir loop oluşmasını engelleyebilmelidir (UDLD)

4.2.20 Anahtar 802.3af ve 802.3at standartlarını desteklemelidir.

4.2.21 Anahtar 48 portundan 15,4 ve en az 24 portundan 30W güç sağlayabilmelidir.

YIGINLAMA

4.2.22 Anahtar yığınlanabilir (stackable) yapıda olmalı veya istenmesi halinde yığınlanabilir hale getirilebilmelidir. Yığınlama için özel yığınlama portları kullanılmalı, kullanıcı veya uplink portları kullanılmamalıdır. Anahtar üzerinde 2 adet yığınlama arayüzü bulunmalı veya istenmesi halinde ayrıca eklenebilmelidir.

4.2.23 En az 8 adet anahtar tek bir yığın içinde bulunabilmelidir.

4.2.24 Yığınlama yapılması halinde, yığındaki anahtarlar arasındaki band genişliği en az 80 Gbps olmalıdır.

4.2.25 Yığınlama yapılması halinde yığın içindeki anahtarlardan birisinin arızalanması durumunda, yığın içindeki diğer anahtarlar çalışmaya devam edebilmelidir.

4.2.26 Yığın tek bir IP adresi üzerinden yönetilebilmeli, yığındaki anahtarların ayrı ayrı yönetilmesi gerekmemelidir.

4.2.27 Yığın içindeki farklı anahtarlara ait portlar tek bir kanal altında toplanabilmelidir. (Cross-stack Etherchannel)

4.2.28 Yığına yeni bir anahtar eklendiğinde otomatik olarak yazılımı güncellenmeli ve herhangi bir konfigürasyon yapılmadan yığının bir üyesi olabilmelidir.

4.2.29 En az 0.5m, 1m ve 3m boyutlarında yığınlama kablosu çeşitliliğine sahip olmalıdır.

SPANNING TREE

4.2.30 Anahtar, IEEE 802.1d, 802.1w ve 802.1s “spanning tree” protokollerini desteklemelidir.

4.2.31 Anahtar üzerinde her VLAN için farklı “spanning tree” kullanılabilmelidir.

4.2.32 Anahtar, kullanıcı ve trunk portlarında spanning tree hesaplarını hızlandırabilmelidir. (Port-fast)

4.2.33 Anahtarın BPDU (Bridge Protocol Data Unit) Guard özelliği bulunacaktır. Bu sayede Spanning Tree grubunda olmayan portlara, o grubun BPDU paketlerinin girişi engellenecektir.

4.2.34 Anahtarın Spanning Tree Root Guard (STRG) özelliği bulunacaktır. Bu sayede network yöneticisinin kontrolünde olmayan anahtarların, Spanning Tree protokolü için root anahtar olması engellenebilecektir.

YÖNLENDİRME

4.2.35 Anahtar statik routing yapabilmelidir. Anahtar üzerinde en az 16 adet statik route tanımlanabilmelidir.

GÜVENLİK

4.2.36 Cihaz, erişim kontrol listeleri ile paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden geçirebilmelidir. Cihaz Erişim Kotrol Listeleri direk olarak L2 veya L3 porta ugulanabileceği gibi VLAN içindeki trafiği de filtreleyebilmelidir. (Router ACL, VLAN ACL, Port-Based ACL)

4.2.37 Anahtar üzerinde bulunan her port için MAC adresi bazında kullanıcı listeleri oluşturulabilmeli ve böylece port güvenliği sağlanabilmelidir. (Port-Security)

4.2.38 Anahtar, MAC adresi tablosuna yeni bir adres eklendiğinde, ya da bu tablodan bir adres silindiğinde, bu durumu SNMP yönetim sunucusuna raporlamalıdır. (MAC Address Notification)

4.2.39 Anahtarın IEEE 802.1x desteği bulunacak ve aşağıda belirtilen 802.1x özellikleri desteklenecektir.

4.2.40 802.1x VLAN assignment; Radius server yardımı ile port bazında kullanıcı yetkilendirme ve dinamik VLAN tahsisi

4.2.41 802.1x Port Security; Port security özelliği, 802.1x etkin bir port üzerinde tanımlanabilmelidir.

4.2.42 802.1x Guest VLAN

4.2.43 802.1x Web yetkilendirmesi

4.2.44 Anahtar, IEEE 802.1x protokolünü kullanarak, radius server yardımı ile port bazında kullanıcı yetkilendirme desteklemelidir. Anahtar, Radius tarafından gönderilen yetkilendirme değişiklik taleplerini yerine getirebilmeilidir. (Change of Authorization)

4.2.45 Anahtarın 802.1X MAC authentication bypass özelliği bulunacaktır.

4.2.46 Anahtar aynı port üzerindeki birden farklı domain'deki cihazların kimlik doğrulama işlemlerini yapabilecektir. Böylece aynı porttaki bir PC ile IP Telefonun ayrı ayrı kimlikleri doğrulayıp uygun veri ve ses VLAN'ilerine atamalarını yapabilecektir. (Multi-Domain Authentication)

4.2.47 IP Spoofing ataklarının engellenebilmesi için, otomatik olarak anahtarın belirtilen portlarına kaynak IP address filtreleri yazılabilecektir (IP Source Guard).

4.2.48 Anahtarın Dynamic ARP Inspection (DAI) özelliği bulunacaktır. Anahtar, üzerinden geçen tüm ARP istek ve cevaplarını incelemeli ve her ARP paketi, IP-MAC binding tablosu ile eşleştirebilmelidir. Eşleşmeyen paketler drop edilebilmelidir.

4.2.49 Erişim seviyesindeki IPv6 adres spoofing, yanlış yönlendirici anonsları gibi IPv6 ataklarını engelleyebilmeldir. (IPv6 First Hop Security)

MULTICAST

4.2.50 Anahtarın multicast desteği olmalıdır. IGMP filtering, ve IGMP Snooping v1-v2-v3, IPv6 MLD v1-v2 snooping desteklenmelidir.

4.2.51 Anahtar, en az 1000 adet IGMP grubu desteklemelidir.

4.2.52 Anahtar, IGMP snooping timer, IGMP throttle, IGMP querier ve Configurable IGMP leave timer özelliklerini desteklemelidir.

GÜÇ TÜKETİM DENETİMİ

4.2.53 Portlardaki trafik yoğnlukları arasındaki sessiz anları belirleyerek, bu zaman aralıklarında portların daha az güç tüketmesini sağlayabilmelidir. (Energy Effıcıent Ethernet)

4.2.54 Anahtar, gece veya haftasonu gibi kullanılmadığı zaman aralıklarında çok düşük güç tüketeceği uyku modunu desteklemelidir. Bu işlem için 'EnergyWise' uyumlu yazılımlar ile uyumlu çalışabilmelidir. (Switch Hibernation Mode)

YÖNETİM ve IZLEME

4.2.55 Anahtarın yalnızca yönetim amacıyla kullanılan 10/100 Mbps Ethernet portu olmalıdır.

4.2.56 Anahtar, SNMP v1, v2, v3, telnet, Secure Shell (SSH), SSL, SCP (Secure Copy Protocol), HTTP (web) ve konsol aracılığı ile yönetilebilmeli veya gözlenebilmelidir.

4.2.57 Anahtarı yönetmek isteyen kişiler Radius sorgulama protokolü tarafından sorgulanabilmelidirler.

4.2.58 TFTP yardımı ile işletim sistemi güncellemesi yapılabilmelidir.

4.2.59 Cihazın tüm portları en az 4 adet RMON grubunu (history, statistics, alarms, events) desteklemelidir.

4.2.60 Detaylı gerçek zamanlı trafik analizi yapabilmek için port mirroring desteği bulunmalıdır. Birden fazla kaynak portu, hedef portuna aynalanabilmelidir. Aynı anda en az 4 adet port mirroring tanımlanabilmelidir.

4.2.61 Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecektir.

4.2.62 Cihaz ile birlikte en az 1 adet 10G SR SFP+ modül teklif edilecektir ve tüm fiber optik modüller aynı üreticinin orijinal ürünleri olmalıdır. OEM parça teklif edilmeyecektir. Teklif edilen kenar anahtarlar Omurga anahtar ile aynı üreticiye ait olmalıdır.

4.3 KABLOSUZ AĞ SİSTEMİ (1 Adet)

4.3.1 Teklif edilen merkez kablosuz ağ kontrol cihazı ve erişim noktası cihazları aynı üreticiye ait olmalıdır.

4.3.2 Teklif edilen kablosuz erişim cihazlarının merkezi yönetimi için kullanılacaktır.

4.3.3 Cihaz, en az 150 adet lokal erişim noktası cihazını destekleyecek donanım yapısına sahip olacak şekilde teklif edilecektir.

4.3.4 Cihaz, en az 25 adet lokal erişim noktası cihazını destekleyecek lisanslama ile teklif edilecektir. İleride lisans arttırımı ile donanım ilavesi yapılmadan en az 150 adet lokal erişim noktası cihazı desteklenebilecektir.

4.3.5 Kablosuz ağ kontrol cihazı üzerinde en az 4 adet 1000BaseT port bulunacaktır. Kablosuz ağ kontrol cihazı Omurga Anahtara en az 1 adet 1000BaseT port üzerinden bağlanacaktır.

4.3.6 Kablosuz ağ kontrol cihazı üzerinde yönetim amaçlı konsol bağlantısı için bir adet konsol portu bulunacaktır.

4.3.7 Cihaz ile, kendisine bağlı olan kablosuz erişim noktalarına güvenlik politikaları uygulanabilmeli, dinamik ve gerçek zamanlı radyo frekanslarının yönetimi, servis kalitesi (QoS) politikaları ve kablosuz IPS özellikleri desteklenmelidir.

4.3.8 Cihaz, RF girişim etkilerine karşı, tespit etme ve önleme özelliklerine sahip olmalıdır.

4.3.9 Cihaz, erişim noktaları arasında yük paylaşımı yaptırabilmelidir.

4.3.10 Cihaz ağın durumuna göre, erişim noktalarının RF çıkış gücünü, dinamik ve gerçek zamanlı olarak ayarlayabilmelidir.

4.3.11 Eğer bir erişim noktası çalışamaz duruma gelirse, cihaz diğer erişim noktalarında gerekli güç ve RF değişikliklerini yaparak çalışmayan erişim noktasının alanını kapsayabilmelidir.

4.3.12 Cihaz IEEE 802.11a, 802.11b, 802.11g ve 802.11n standartlarını destekleyecektir.

4.3.13 Cihaz üzerinde IEEE 802.1Q desteği olmalıdır.

4.3.14 IEEE 802.1X standardını desteklemelidir. IEEE 802.1X desteği olmayan istemciler için web tabanlı yetkilendirme yapabilmelidir.

4.3.15 Misafir VLAN desteği olmalıdır. IEEE 802.1X yetkilendirmesinde başarısız olan istemcileri, otomatik olarak kısıtlı bir VLAN'a atayabilmelidir.

4.3.16 Misafir VLAN'a bağlanabilmek için gerekli misafir kimlik bilgileri, yetkilendirilecek yöneticiler tarafından tanımlanabilmesine olanak sağlayan ayrı bir Web yönetim arayüzü bulunacaktır. Sistem bu altyapıyı, ek bir donanım veya yazılıma gereksinim olmaksızın destekleyebilmelidir.

4.3.17 Misafir kullanıcılar için, misafir VLAN'ina erişim sağlamadan önce Web tabanlı yetkilendirme yapabilmelidir.

4.3.18 Misafir VLAN'a bağlanacak kullanıcıların tanımlanacak bir web sayfasına yönlendirilmesi sağlanacaktır.

4.3.19 İstendiği takdirde misafir VLAN'ine ait trafiği doğrudan DMZ bölgesine yönlendirebilmelidir.

4.3.20 WEP, WPA ve WPA2 desteği olmalıdır.

4.3.21 Kriptolama için AES ve IPSEC desteği olmalıdır.

4.3.22 Harici bir RADIUS ve/veya TACACS sunucusu üzerinden, kullanıcıların kimlik sorgulamasını yapabilmelidir. (Kurum LDAP yapısı ile entegre edilecektir).

4.3.23 Kablosuz ağ kontrol cihazı, istenmesi durumunda N+1 modunda yedekli çalışmayı desteklemelidir.

4.3.24 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 kayıt olabilmelidir.

4.3.25 Kablosuz ağ kontrol cihazı, uzak bölgelerde bulunan erişim noktalarını yönetebilmelidir.

4.3.26 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.

4.4 KABLOSUZ ERİŞİM CİHAZI (25 Adet)

4.4.1 Önerilecek olan kablosuz ağ cihazı (kablosuz erişim noktası), 2,4 ve 5 GHz frekans bandında çalışabilecektir.

4.4.2 Kablosuz erişim noktası, teklif edilen merkez kablosuz ağ kontrol cihazı tarafından yönetilebilmelidir.

4.4.3 Kablosuz erişim noktası üzerindeki kullanıcı trafiği, merkez kablosuz ağ kontrol cihazı üzerinden, ağa iletilmelidir.

4.4.4 Cihaz, kablosuz kontrol cihazı tarafından yönetilip istenilen ssidlerin trafiğini merkezi, istenilen ssidlerin trafiği lokal olarak anahtarlayabilmelidir.

4.4.5 Kablosuz erişim noktası, 2.4Ghz bandında ETSI standartlarında 13 adet çalışma kanalını desteklemelidir. 3 adet kablosuz erişim noktası aynı ortamda yan yana frekans örtüşmesi olmadan çalışabilmelidir.

4.4.6 Kablosuz erişim noktası, IEEE 802.11ac, IEEE 802.11n, IEEE 802.11a IEEE 802.11b ve IEEE 802.11g standartlarını tam uyumlu olarak destekleyecektir.

4.4.7 Cihaz üzerindeki kullanıcılar maksimum 1.3 Gbps hıza ulaşabilmelidir.

4.4.8 Kablosuz erişim noktası, IEEE 802.11n için, 4x4 multiple-input, multiple-output (MIMO), 3 spetial streams, 802.11 dynamic frequency selection (DFS), maximal ratio combining (MRC), cyclic shift diversity (CSD) ve 20 , 40 ve 80 MHz kanallarını desteklemelidir.

4.4.9 Cihaz üzerinde spectrum analyzer donanımı bulunmalıdır. Bu donanım üzerinden alınan bilgiler ile wireless enterferansa karşı self healing ve optimizasyon yapılabilmelidir.

4.4.10 İstenildiği takdirde cihaz üzerine spektrum analizi için ayrı antenler içeren bir modül takılıp tüm donanım fiziksel olarak ayrılabilmelidir. Eğer bu özellik desteklenmiyorsa her bir erişim noktası için 1 adet de sadece monitör modunda çalışacak bir erişim noktası teklif edilmelidir.

4.4.11 Cihaz üzerinde spectrum analyzer tek başına site survey amacıyla kullanılabilmeli, uzakdaki makinede kurulan Spectrum Expert yazılımının sensoru şeklinde çalışabilmelidir.

4.4.12 Cihaz Kablosuz saldırı engelleme sistemelerinin sensoru şeklinde de çalışabilmedilir. Bu şekilde çalışırken üzerine kullanıcı almaya devam edebilmelidir.

4.4.13 Cihaz 802.11a/g/n kullanıcıların performansını arttırmak için Clientlink özelliğini desteklemelidir.

4.4.14 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.

4.4.15 Kablosuz erişim noktası, hızlı roaming özelliklerine sahip olmalıdır.

4.4.16 Kablosuz erişim noktası üzerinde, 1 adet 10/100/1000BASE-T portu (RJ-45) bulunmalıdır.

4.4.17 Kablosuz erişim noktası, 48 V DC güç kaynağı ile çalıştırılabilmeli, ya da IEEE 802.3af veya benzeri bir yöntemle, UTP kablo üzerinden de beslenebilmelidir.

4.4.18 Cihazın çıkış gücü (transmit power), ETSI standartlarına uygun olmalıdır. Gerektiğinde çıkış gücü, daha düşük bir seviyeye ayarlanabilmelidir.

4.4.19 Kablosuz erişim noktası üzerinde, 2.4 Ghz için entegre 4.0 dBi kazançlı, 5 Ghz için entegre 6.0 dBi kazançlı, omni-directional (yaklaşık 360º) anten bulunmalıdır.

4.4.20 Kablosuz erişim noktası üzerinde, IEEE 802.1Q VLAN tagging (VLAN trunking) desteği bulunmalıdır.

4.4.21 Kablosuz erişim noktası üzerinde, en az 16 adet VLAN (Virtual LAN) tanımlanabilmelidir.

4.4.22 Kablosuz erişim noktası üzerinde, en az 16 adet SSID (service set identifier) tanımlanabilmeli ve her VLAN için farklı SSID tahsis edilebilmelidir.

4.4.23 Kablosuz erişim noktası, IEEE 802.1p önceliklendirme standartını desteklemelidir.

4.4.24 Kablosuz erişim noktası üzerinde, işletim sistemi ve konfigürasyon dosyalarını tutmak vb. Amacıyla, 512MB RAM ve 64 MB flash bellek bulunmalıdır.

4.4.25 Kablosuz erişim noktası, 40 ve 128 bit uzunluğundaki IEEE 802.11 WEP şifrelerini (key) desteklemelidir.

4.4.26 Kablosuz erişim noktası, Wi-Fi Protected Access (WPA) ve WPA2 sertifikasyon yöntemlerini desteklemelidir. WPA için TKIP (temporal key integrity protocol) ve WPA2 için AES (advanced encryption standart) şifreleme desteği bulunmalıdır.

4.4.27 Kablosuz erişim noktası, IEEE 802.1x authentication desteğine sahip olmalıdır.

4.4.28 Kablosuz erişim noktası, IEEE 802.11i güvenlik standartını desteklemelidir.

4.4.29 Kablosuz erişim noktası üzerinde, cihazın durumunu, ethernet bağlantısının durumunu ve aktivitesini, kablosuz bağlantının durumunu ve aktivitesini ayrı ayrı gösteren LED ler bulunmalıdır.

4.4.30 Kablosuz erişim noktası üzerindeki konfigürasyon, gerektiğinde tek bir butona basarak silinebilmeli ve fabrika çıkış değerlerine dönülebilmelidir.

4.4.31 Cihazın duvara, tavana ya da masa üstüne monte edilmesini sağlayan kitler birlikte verilecektir. Cihaz, kilitlenebilmeli ve monte edildiği yerden hırsızlık vb. nedenlerle sökülmesi engellenebilmelidir.

4.4.32 Cihazın çevre sıcaklığı, 0 ºC / +40 ºC arasında olmalıdır. %10 / %90 nem aralığında çalışabilmelidir.

4.4.33 Teklif edilen cihaz Kablosuz Ağ Sistemi ile aynı üreticiye ait olmalıdır.

4.5 AĞ ERİŞİM KONTROL SİSTEMİ (1 Adet)

4.5.1 Teklif edilecek sistem, en az politika yöneticisi, uygulayıcı sistemler ve istemci ajanı bileşenlerinden oluşmalıdır ve kimlik denetimi, yetkilendirme, uyumluluk kontrolü, misafir erişimi, yönetimi ve izlenmesi ve cihazların otomatik olarak trafik tiplerine göre profillendirmesi, sonrasında ise tanımlı rollere atanması işlemlerini birbiri ile tamamen uyumlu bir şekilde sağlamalıdır.

4.5.2 Ağ erişim kontrol sistemi aynı üreticinin sağladığı “Uygulama ve Ağ Performans Yönetim ve Analiz Sistemi” ile entegre ve uyumlu çalışmalıdır.

4.5.3 Teklif edilecek sistem, yönetim, raporlama ve politika ve kural tanımlama fonksiyonlarını sağlayacaktır.

4.5.4 Teklif edilecek sistem üzerinde tüm yetkilendirme ve izin verme süreci detaylı olarak loglanacak ve bu loglar üzerinde tüm süreç takip edilebilecektir.

4.5.5 Kurumsal Ağ altyapısına erişmek için girişimde bulunan tüm son kullanıcı cihazlarına (kişisel bilgisayar, Tablet, Cep telefonu, printer, IP Telefon, IP fax, IP kamera gibi), Kurumsal güvenlik politikası uyumluluğuna göre dinamik olarak erişim izni verilecek yada engellenecektir.

4.5.6 Kablosuz ağ üzerinden erişim girişiminde bulunan kullanıcı cihazları için güvenlik politikası uyumluluğu kontrol edilebilecek ve uyumlu olan kullanıcı cihazlarına erişim izni verilecek, uyumsuz olanlar ise engellenecektir. Bu özellik kablolu ve VPN üzerinden gelen kullanıcı cihazları ve kullanıcılar için de sağlanabilecektir.

4.5.7 Teklif edilecek sistem son kullanıcı cihazlarına dinamik olarak profil atayabilecektir. Bu profillendirmeyi Radius , MAC adresi , DHCP opsiyon , DNS hostname ve HTTP user agent vb. tabanlı olarak yapabilecektir.

4.5.8 Son kullanıcı cihazları için profiller yada roller, her profil yada rol için farklı kurallar ve her kural için de farklı kontroller tanımlanabilecektir.

4.5.9 Son kullanıcı cihazlarına, cihaz tipine ve marka modeline göre farklı profil veya rol atanabilecektir.

4.5.10 Kullanıcılara, Kurum için de çalıştıklara bölüme bağlı olarak farklı roller atanabilecektir (bilgi işlem, finans, personel vb.).

4.5.11 Misafir kullanıcılar için Agentless (ajansız) Web tabanlı kimlik doğrulama ve sonrasında yetkilendirme desteklenecektir.

4.5.12 Aynı anda birden fazla kimlik doğrulama sunucusunu desteklenecektir.

4.5.13 Yönetim sunucusunun detaylı raporlama özellikleri bulunacak ve istenmesi durumunda bu raporlar API'ler ile harici bir sunucuya ya da kayıt ortamına alınıp saklanabilecektir.

4.5.14 Yönetim sunucusu üzerinden merkezi olarak alınacak raporlar aşağıda belirtilen bilgileri içerecektir.

4.5.15 Kimlik doğrulamadan geçen kullanıcılar

4.5.16 Kimlik doğrulamadan geçemeyen kullanıcılar

4.5.17 Tanımlanan kurallardan geçen kullanıcılar

4.5.18 Tanımlanan kurallardan geçemeyen kullanıcılar

4.5.19 Tanımlanan kurallardan geçemeyen kullanıcıların hangi kuraldan/kurallardan dolayı geçemedikleri

4.5.20 Tarih (gün.ay.yıl) ve zaman (saat:dakika:saniye) bilgisi

4.5.21 Oluşturulan profillerdeki online cihazlar

4.5.22 Cihazın MAC ve varsa IP adresi

4.5.23 Cihazın etkisi altında olduğu uygulayıcı

4.5.24 Kullanıcı bilgisayarının işletim sistemi

4.5.25 Kullanıcı bilgisayarında ajan olup olmadığı

4.5.26 Her bir Kurum kullanıcısına Active Directory entegrasyonu ile misafirlere, misafir erişim hakkı vermesi sağlanacaktır. Ayrıca istenmesi durumunda tanımlanacak sistem yöneticilerine sadece misafir erişim hakkı açma yetkisi verilmiş kullanıcıların açtıkları misafir erişim haklarını izleme, raporlama ve sonlandırma yetkisi sağlanacaktır.

4.5.27 Misafir erişiminin açılması için kullanılacak web sayfasından, ağ erişim kontrol sistemine konfigurasyonlarına kesinlikle ulşılamıyacak. Kurum kullanıcısı sadece misafir kullanıcı açmak için gerekli alanları görebilecektir.

4.5.28 Misafir erişimi için misafir kullanıcı bilgileri (misafir kullanıcı adı ve misafir kullanici şifresi), misafire text olarak verilebilecek ve istenmesi durumunda e-mail ile de gönderilebilecektir.

4.5.29 Misafir kullanıcılara açılacak erişim hakkı yıl, ay, gün, saat ,dakika olarak tanımlanabilecek ve tanımlanan sure sonunda erişim hakkı sistem tarafından otomatik olarak sonlandırılacaktır. Ayrıca, tanımlanan misafir erişim hakkı herhangi bir anda erişim hakkını tanımlayan kullanıcı tarafından sonlandırılabilecektir.

4.5.30 Tekli yada çoklu misafir (aynı anda birden fazla kullanıcı için) erişim hakkı tanımlaması yapılabilecektir.

4.5.31 Çoklu erişim hakkı tanımlaması özel olarak hazırlanacak ve kullanıcı bilgilerini içeren bir dosyanın yüklenmesi ile de sağlanabilecektir.

4.5.32 Misafir kullanıcılara erişim hakları, kimin tarafından erişim hakkı açıldığı ve erişim tanımları izlenebilecek ve raporlanabilecektir.

4.5.33 Son kullanıcı kişisel bilgisayarlarında aşağıda belirtilen tarama ve kontroller yapılabilecektir.

4.5.34 Microsoft tabanlı İşletim Sisteminin tipi

4.5.35 Microsoft tabanlı İşletim Sisteminin servis tipi

4.5.36 Microsoft tabanlı İşletim Sisteminin güncelliği

4.5.37 Antivirus yazılımının yüklü olup olmadığı

4.5.38 Antivirus yazılımının güncelliği, marka bağımsız olarak versiyon kontrolü yapabilmeli, ilgili antivirus yazılımının bir ay dan daha eski olup olmadığını kontrol edebilmelidir.

4.5.39 Bilgisayarda o anda çalışmakta olan servisler

4.5.40 Bilgisayarda o anda çalışmakta olan uygulamalar

4.5.41 İstenilen uygulamanın o anda çalışıp çalışmadığı

4.5.42 Bilgisayarın registry (kütük)'sindeki alanlar

4.5.43 Bilgisayarın hard diskindeki dosyalar

4.5.44 Ağ erişim kontrol sistemi ile bir adet sanal sunucu lisansı, 3000 Baz Lisans ve Plus Lisans, Apex Lisans ise sayısı 499 adet olarak teklif edilecektir. Teklif içerisinde TACACS lisansı da teklif edilecektir.

4.5.45 Sistem 1 senelik üretici destek lisansı dahil teklif edilecektir.

4.5.46 Teklif edilecek Ağ Kontrol Sistemi, mevcutta bulunan network alt yapısı ile birebir uyumlu olacaktır.

4.6 DNS KATMANI GÜVENLİK ÇÖZÜMÜ (1 Yazılım 250 Kullanıcı)

Mimari

4.6.1 Teklif edilecek çözüm recursive DNS Analizi yapmalıdır.

4.6.2 Teklif edilecek çözüm herhangi bir fiziksel donanım kurulumu gerektirmeyen, mevcut DNS altyapısı üzerinde minimum işlem yapılarak çalışmalıdır.

4.6.3 Teklif edilecek çözüm, ek fiziksel donanım maliyeti gerektirmeden, DNS Sunucusu üzerine forwarder tanımlaması yapılarak, internal sanal forwarder kurularak vb. gibi farklı kurulum seçenekleri sunmalıdır.

4.6.4 Recursive DNS Servisi, global veri merkezi networkleri üzerinden sağlanmalıdır

4.6.5 Teklif edilecek çözüm ile, kablolu ve kablosuz ağlardan bağlanan kurumsal kullanıcılara eş zamanlı olarak uygulanabilmeli, farklı public IP'lere ve iç ağlara veya Active Directory kullanıcılarına göre farklı politikalar tanımlanabilmelidir

4.6.6 Teklif edilecek çözümün API desteği olmalıdır. Bunun için ek lisans gerekiyor ise isteğe bağlı olarak teklif edilmelidir.

4.6.7 Son kullanıcılar için korumanın her yerde devamının sağlanabilmesi için ajan kurularak korumanın devam ettirilmesine olanak sağlamalıdır.

4.6.8 3.party üreticiler ile entegre olabilmelidir. Bunun için ek lisans gerekiyor ise isteğe bağlı olarak teklif edilmelidir.

Güvenlik

4.6.9 Teklif edilecek çözüm, kötü amaçlı yazılımlar(malware) tarafından kullanılan spesifik port ve protokol bağımsız olarak, gelişmiş kötü amaçlı yazılımları(malware) tespit ve engelleme yeteneğine sahip olmalıdır.

4.6.10 Çözüm, HTTP / HTTPS'den farklı protokolleri kullanan kötü amaçlı yazılımları tespit edip engelleyebilmelidir.

4.6.11 Çözüm, özel bir kurum için hedeflenmiş, gelişmiş malware saldırılarını tespit edip engelleyebilmelidir.

4.6.12 Çözüm en az botnets, phishing saldırıları, vpn dns tunellemeleri ve cryptomining gibi malware kategorilerine karşı koruma sağlayabilmelidir.

4.6.13 Çözüm Dinamik DNS hizmetlerine yönlendirilen şüpheli DNS isteklerini algılayabilmeli ve engelleyebilmelidir.

4.6.14 Çözüm sadece statik imzalar ve kara listelere bağlı kalmadan, istihbarat merkezinden (threat intelligence) bilgi alabilmelidir.

4.6.15 Çözümün dünyada en az 25 lokasyonda hizmet veren veri merkezleri bulunmalıdır.

4.6.16 Kötü amaçlı yazılım(malware) tespitini küresel ölçekte sağlamak için, tehdit istihbaratı (threat intelligence) oluşturmak için kullanılan ağ, en az günlük 60 milyon kullanıcıdan en az günlük 80 milyon DNS isteğini işlemelidir.

4.6.17 Analiz algoritmaları çok katmanlı aşağıdaki gibi dedektörler kullanmalıdır.

4.6.18 DNS co-occurrences Analizi

4.6.19 Domain tabanlı Natural Language Processing Algoritma Analizi

4.6.20 DGA (Domain Generated Algorithm) Tespiti

4.6.21 DNS Peak Trafik Tespiti

4.6.22 Tahminsel IP Aralığı Analizi (Predictive IPS Space Modelling)

4.6.23 İstihbarat Merkezi (Threat Intelligence) herhangi bir manuel güncelleme işlemi olmaksızın yeni bir tehdidin bulunmasından 15 dakika sonra otomatik olarak güncellenmelidir.

4.6.24 Çözüm, transparan proxy özelliği ile http ve HTTPS trafiklerini kontrol edebilmelidir. Transparan proxy kullanımı için herhangi bir proxy pac dosyasının kullanımına ihtiyaç duymamalıdır.

4.6.25 Çözüm, en az 60 kategoriye dayanan Web filtreleme özelliğine sahip olmalıdır. Web filtreleme politikasını bağımsız olarak güvenlik politikasını oluşturmak mümkün olmalıdır.

4.6.26 Web filtreleme ve güvenlik politikaları, özel beyaz ve kara listeler tanımlanarak istisnalar oluşturulmasına izin vermelidir.

4.6.27 Çözüm, uygulama kontrol özelliğine sahip olmalı ve uygulamaya bağlı kuralların tanımlanarak, istenilen uygulamaların engellenmesine olanak sağlamalıdır.

Yönetim

4.6.28 Yönetim arayüzü web-tabanlı olmalı ve multi-tenant mimariye uygun olmalıdır. Farklı profillerde ve rollerde kullanıcı tanımlamasına izin vermelidir. (Örnek : Administrator, Reporting User, Read-Only User)

4.6.29 Yönetim arayüzü, güvenlik ve web filtreleme politikalarını tanımlamak için grafiksel kural editörü sağlamalıdır.

4.6.30 Network, kullanıcılar, bilgisayarlar gibi kimliklere dayalı güvenlik politikalarının oluşturulmasına izin vermelidir.

4.6.31 Güvenlik kuralları farklı güvenlik ve web filtreleme profillerinin oluşturulmasına izin vermelidir.

4.6.32 Engellenen DNS bağlantıları için bir engelleme sayfası tanımlamaya izin vermelidir.

4.6.33 Her politika girişi için engelleme sayfasını özelleştirmek mümkün olmalıdır. Özelleştirme, özel bir mesaj tanımlama, özel logo veya yönetici e-posta adresi ekleme yeteneğini içermelidir.

4.6.34 Kural yazımı engellenen bağlantıyı dahili bir URL'ye iletmeye izin vermelidir.

4.6.35 Sistem, engelleme sayfasını atlayabilme özelliğine sahip yerel bir veritabanında kullanıcı oluşturmaya(bypass user) izin vermelidir.

4.6.36 Kullanıcılar için engelleme sayfalarını atlamaya izin veren özel kodlar(bypass codes) oluşturmaya izin vermelidir.

4.6.37 Analiz edilen tüm DNS sorgularıyla ilgili olaylar, filtrelere kimlik, hedef, kaynak IP, yanıt tipi ve tarih bazında gerçek zamanlı olarak görünmelidir.

4.6.38 Tüm filtreler, özel bir zaman tanımlamak için geçerli olmalıdır (tarihe göre filtrele).

4.6.39 Tüm filtreler, web filtreleme kategorilerini ve / veya güvenlik kategorilerini seçerek uygulanabilir olmalıdır.

4.6.40 Dashboard hedefli saldırıları tanımlamak için yapılandırılmış her bir sitede genel DNS etkinliğini gösterebilmelidir

4.6.41 Yönetim platformu gelişmiş raporlama yeteneklerine sahip olmalıdır.

4.6.42 Yönetim platformu en az aşağıdaki rapor tiplerinde raporların oluşturulmasına imkan sağlamalıdır.

4.6.43 Toplam Istek (Total Request)

4.6.44 Aktivite Boyutu (Activity Volume)

4.6.45 Top Domains

4.6.46 Top Categories

4.6.47 Top Identities

4.6.48 Tüm raporlar csv formatında export edilebilmeli ve otomatik olarak email gönderilebilmelidir.

4.6.49 Teklif edilecek çözüm kurum altyapısında 1000 IP adresi için 1 yıllık üretici destek paketi dahil şekilde yüklenici firma tarafında tekliflendirilmelidir.

EK ALIM;

Mevcutta kullanılan Cisco marka UC platformu için lisans ve IP telefon alımı olacaktır. Ek alım kısmı da projeye dahil edilecektir. İhtiyaç listesi aşağıdaki gibidir.

AÇIKLAMA	ADET
UC Manager-10.x Enhanced Single User License	96
Cisco UC Phone 7841	70
Cisco Unified Wireless IP Phone 8821, World Mode Bundle	10
Cisco IP Phone 8851	1

5 GÜVENLİK TEKNİK GEREKSİNİMLERİ

5.1 AĞ GÜVENLİK CİHAZI (2 Adet)

5.1.1 Teklif edilecek 'Ağ Güvenlik Duvarı Sistemi' asgari olarak aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.

5.1.2 Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;

5.1.3 Güvenlik Duvarı (Firewall)

5.1.4 IPSec VPN Sonlandırma Sistemi

5.1.5 SSL VPN Sonlandırma Sistemi

5.1.6 Saldırı Tespit ve Engelleme Sistemi (IPS)

5.1.7 Uygulama Tanıma ve Kontrolü (Application Control) Sistemi

5.1.8 Virüs/Zararlı İçerik Kontrolü

5.1.9 URL Kategori Filtreleme

5.1.10 Bant genişliği yönetimi özelliklerine sahip olmalıdır.

5.1.11 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.

5.1.12 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.

5.1.13 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.

5.1.14 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.

5.1.15 Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.

5.1.16 Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır.

5.1.17 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.

5.1.18 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.

5.1.19 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.

5.1.20 Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;

5.1.21 SPI (stateful packet inspection),

5.1.22 Saldırı Tespit ve Engelleme Sistemi (IPS)

5.1.23 Uygulama Tanıma ve Kontrolü (Application Control) Sistemi

5.1.24 Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü

5.1.25 URL Kategori Filtreleme

5.1.26 Routing modda aşağıdaki özellikleri sağlamalıdır;

5.1.27 SPI (stateful packet inspection),

5.1.28 IPSec VPN Sonlandırma,

5.1.29 SSL VPN Sonlandırma,

5.1.30 Saldırı Tespit ve Engelleme Sistemi (IPS)

5.1.31 Uygulama Tanıma ve Kontrolü (Application Control) Sistemi

5.1.32 Virüs/Zararlı İçerik Kontrolü

5.1.33 URL Kategori Filtreleme

5.1.34 Bant genişliği kontrolü

5.1.35 Statik yönlendirme (static routing),

5.1.36 RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.

5.1.37 Sunucu yük dengeleme

5.1.38 WIFI Access Point kontrolcüsü

5.1.39 WAN optimizasyon

5.1.40 Web Cache

5.1.41 Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.

5.1.42 Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.

5.1.43 Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.

5.1.44 Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü ve/veya zone bazlı yazılabilmelidir.

5.1.45 Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.

5.1.46 Kullanıcı bazında NAT kuralı yazılabilmelidir.

5.1.47 Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.

5.1.48 Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.

5.1.49 Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.

5.1.50 İstenildiğinde tek IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural dahilinde izin verilmiş olan tüm kaynak IP lerin herbiri için, tanımlanan bant genişliğinin ve/veya max eşzamanlı oturum sayısının garanti edilmesi sağlanmalıdır.

5.1.51 Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.

5.1.52 Uygulama bazında bant genişliği kontrolü yapabilmelidir.

5.1.53 Aynı trafik ile ilgili Inbound ve outbound doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.

5.1.54 Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

5.1.55 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.

5.1.56 Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.

5.1.57 Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.

5.1.58 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.

5.1.59 Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapan IP adresinin olası diğer saldırıları başlamadan engellenmiş olmalıdır.

5.1.60 Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkân sağlamalıdır.

5.1.61 Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.

5.1.62 Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.

5.1.63 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.

5.1.64 SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.

5.1.65 SSL VPN özelliği minimum 10.000 kullanıcı lisansı ile teklif edilecektir.

5.1.66 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.

5.1.67 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.

5.1.68 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

5.1.69 Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.

5.1.70 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.

5.1.71 Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı URL filtreleme politikaları set edilebilmelidir.

5.1.72 Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.

5.1.73 Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.

5.1.74 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 YIL geçerli olacak şekilde teklif edilmelidir.

5.1.75 URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.

5.1.76 İstenildiğinde categorilerden bağımsız olarak, sisteme eklenebilecek tam URL bilgisi (Örneğin: www.abc.com/deneme/sayfa1.php) bazında engelleme yapabilmelidir.

5.1.77 Https üzerinden erişilmeye çalışılan domain adreslerinin (örneğin www.abc.com) engellemesi sertifika kullanımı olmadan gerçekleştirilebilmelidir.

5.1.78 SSL trafiğini kendi üzerinde yaratılan bir sertifikayı yada farklı bir CA den alınmış yeterli özelliklere sahip bir sertifika ile inceleyebilmelidir. Bu sayede sadece domain bazında değil, URL bazında (Örneğin: www.abc.com/deneme/test.php) engelleme yapabilmelidir. URL kategorileri bazında SSL incelemeye girmeyecek domainler belirlenebilmelidir.

5.1.79 URL filtreleme uyarı ekranları özelleştirilebilecektir.

5.1.80 Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir.

5.1.81 Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:

5.1.82 Seri bağlantı ile konsol port üzerinden,

5.1.83 Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden

5.1.84 SSH bağlantı ile komut satırı (commandline) üzerinden

5.1.85 Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir

5.1.86 Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

5.1.87 Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.

5.1.88 Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, "NSS Labs Network IPS" ve "NSS Labs Next Generation Firewall" testlerine girmiş olması gereklidir.

5.1.89 Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel "Enterprise Firewall" için "Gartner Magic Quadrant" tablosunda yer almalıdır.

5.1.90 Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.

5.1.91 Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.

5.1.92 Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP, Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.

5.1.93 Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.

5.1.94 HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.

5.1.95 SSL bağlantıları için SSL Offloading özelliği olmalıdır.

5.1.96 Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:

5.1.97 Kaynak Ip hash bilgisi

5.1.98 Round robin

5.1.99 Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak

5.1.100 Aktif durumda olan gerçek sunuculardan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi

5.1.101 Ping paketlerine verilen cevaplar esas alınması

5.1.102 Sunucular üzerine yönlendirilen session (oturum)sayı bilgisine bağlı olarak

5.1.103 Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin http://10.31.101.30/test_page.htm adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.

5.1.104 Teklif edilen sistem wifi controller olarak çalışabilecek, bu sayede kullanılabilecek kablosuz erişim cihazlarının yönetimi için kullanılabilecektir.

5.1.105 Teklif edilen sistem WAN optimizasyon özelliklerine sahip olacaktır.

Güvenlik Duvarı Performans Değerleri

5.1.106 Teklif edilen Ağ Güvenlik Duvarı, yedekli çalıştırılacak şekilde **2 adet teklif edilecektir**, Her iki cihaz üzerinde (Firewall + IPS + Uygulama Denetimi + Antivirüs + İçerik Filtreleme + Cloud Sandboxing) gibi özellikler üretici destek lisansına dahil edilmelidir.

5.1.107 Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, en az 55 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.

5.1.108 Her bir Ağ Güvenlik Duvarı ünitesi/kartı (cluster içerisindeki herbir cihaz/kart ayrı ayrı olmak üzere) Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az 5 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 7 Gbps olmalıdır.

5.1.109 Sistem aynı anda en az 12 milyon oturumu desteklemeli ve saniyede en az 300.000 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.

5.1.110 Güvenlik Duvarı Sistemi en az 50 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.

5.1.111 Güvenlik Duvarı Sistemi en az 4.0 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.

5.1.112 Sistem Site-to-Site için en az 20.000 adet, Client to site için 50.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir

5.1.113 Sistem 13 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.

5.1.114 Sistem üzerinde;

5.1.115 En az 16 adet 1GE RJ45 ara yüz bulunmalıdır.

5.1.116 En az 16 adet 1GE SFP ara yüz bulunmalıdır.

5.1.117 En az 8 adet 10GE SFP+ ara yüz bulunmalıdır.

5.1.118 Güvenlik Sistemi üzerinde en az 450 Gbyte kapasitede depolama alanı bulunmalıdır. Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama Sistemine kayıt gönderebilmeli ve sistem üzerindeki Depolama Biriminde de kayıt Tutabilmelidir.

5.1.119 Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri 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, Cloud Sandboxing , Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

5.2 YÜK DENGELEME CİHAZI (2 Adet)

5.2.1 Kurum, Sunucu Yük Dengeleme ve Uygulama Güvenlik Duvarı çözümlerini tek bir platformda yazılım ve donanım bütünü (appliance) olarak satın alacaktır.

5.2.2 Cihaz Genel Özellikleri

5.2.3 Sistem, iki cihaz Aktif/Aktif ya da Aktif/Pasif yedekli yapıyı desteklemelidir. Kuruma bu yapıyı destekleyecek birbirinin aynı olan iki cihaz teklif edilecektir. İki veya daha fazla cihaz olan Aktif-Aktif yapıda cluster olarak çalışırken, şartnamede belirtilen tüm fonksiyonlar sistem üzerinde eksiksiz sağlanmaya devam edilmelidir.

5.2.4 Teklif edilecek olan yük dengeleme cihazı 1 yıl boyunca cluster mimaride her iki fiziksel yük dengeleme cihazı için 1 yıllık üretici destek paketi içerecektir.

5.2.5 Cihaz yedek çalışabilen 2 adet AC güç kaynağını desteklemelidir.

5.2.6 Sistem üzerinde aynı anda farklı versiyon yazılım imajı kurulabilmelidir. Sistemin default olarak yüklü imajlardan hangisi ile açılacağı belirlenebilmelidir. Ayrıca istenmesi durumunda sistemin açılışı sırasında konsoldan bağlanarak, yüklü imajlardan hangisi ile boot edileceği de seçilebilmelidir. Bu sayede versiyon yükseltme sonrası problem yaşanması durumunda bir önceki versiyon ile sistemi açabilmek mümkün olmalıdır.

5.2.7 Sistem USB portuna bağlanacak harici disk üzerinden boot edilebilmelidir. Gerekmesi durumunda sisteme yeni imaj kurulumu boot edilen harici disk üzerinden yapılabilmelidir.

5.2.8 Cihaz üzerinde en az 1 adet 2-core işlemci bulunmalıdır.

5.2.9 Cihazda 16 GB RAM bulunmalıdır.

5.2.10 Cihaz üzerinde en az 4 adet 1 Gbps ve 2 adet 10Gbps arayüz bulunmalıdır. Cihaz üzerinde 2 adet 1000Mbps bakır arayüzü ve 2 adet 10Gbps SR takılı gelmelidir.

5.2.11 Cihazın üzerinde SSL şifreleme için özel kart donanımı bulunmalıdır

5.2.12 Web ara yüzü üzerinden raporlama ve istatistiksel veri izleme yapılabilmelidir.

5.2.13 Farklı yetkilere sahip kullanıcı tanımlamaları yapılabilmelidir.

5.2.14 Cihaz konfigürasyonu harici bir ortama yedeklenebilmeli ve gerektiğinde yeniden yüklenebilmelidir.

5.2.15 Sistemin alınan konfigürasyon yedeği, gerekmesi durumunda firmanın farklı donanım modeline sahip cihazlarına da dönülebilmeli ve aynı şekilde konfigüre edilmiş, tüm fonsiyonları sağlayacak şekilde sistemi çalışır hale getirebilmelidir.

5.2.16 İşletim sistemi yükseltme veya önceki sürüme dönme işlemleri web ara yüzünden yönetilebilmelidir.

5.2.17 Sistem üzerinde yönetim için ayrı bir ağ bağlantısı olmalı ve out-of-band yönetim yapılabilmelidir. Yönetim için sisteme verilen IP adresine özel ayrı bir default gateway (default route) tanımlanabilmelidir.

5.2.18 Sistemin donanım tanı (hardware diagnostic) desteği bulunmalıdır. Bunun için gerekli yazılım bileşenleri sistem üzerinde yüklü gelmelidir. Son kullanıcı, donanım tanı işlemini kendisi sistem üzerinde yapabilmelidir. İstendiği durumda donanım tanı bilgileri online olarak üretici firma web sitesine yüklenerek, daha detaylı olarak gerçek zamanlı analiz ve tanı kullanınıcının kendisi tarafından yapılabilmelidir.

5.2.19 Sistem üzerinde, aktif-pasif yapıda çalışırken hata geçişi (failover) için diğer cihazla haberleşmesini sağlayacak özel serial-failover portu bulunmalıdır. Bu sayede bir saniyenin altında hata geçişine (failover) imkan verebilmelidir.

5.2.20 Cihazlarda, SNMP v1, SNMP v2 ve SNMP v3 desteği bulunacaktır.

5.2.21 Cihazlar, SNMP trap ile üzerindeki up/down olayını, başka bir yönetim sistemine iletmesi sağlanacaktır.

5.2.22 Cihazlar, SNMP tabanlı sistemler ile entegre edilecektir. Yüklenici, cihazla etkileşim için SNMP MIB dosyalarını sağlayacaktır.

5.2.23 Cihazlarda, canlı performans, erişilebilirlik ve istatistikî bilgiler grafik ara yüzünden takip edilmesi sağlanacaktır. Bunun için gerekli lisanslar sistem üzerinde yüklü gelmelidir.

5.2.24 Sistem üzerinde tanımlanan web servisleri için arka taraftaki sunucudan cevap dönüş süresi (server latency), uygulama sayfasının yükleme süresi (Application Page Load Time), erişilen URL listesi, erişen kullanıcıların IP adresleri, saniyedeki işlem miktarı (Transaction Per Second), istek için ve cevap için (request ve response) ayrı olarak bandgenişliği kullanımı (throughput), hangi ülkeden erişim sağlandığı, kullanıcı isteğine dönen cevap kodu (response code), kullanıcı tarayıcısı ve istek içindeki HTTP metodu bilgileri kullanıcı oturumları bazında (unique user session) izlenip geriye yönelik görsel olarak raporlanabilmelidir. Raporlar belirlenen email adresine otomatik ve düzenli olarak PDF veya CSV formatında email ile gönderilebilmelidir. İzlenen ve raporlanan parametreler ile ilgili belirlenen kriterlerin aşılması durumunda sistem otomatik olarak bilgilendirme mesajları (E-mail, syslog ya da SNMP trap olarak) gönderebilmelidir. Bu fonksiyonların sağlanması için gerekli tüm lisanslar sistem üzerinde yüklü gelmelidir. Eğer sistem bu fonksiyonları kendi üzerinde sağlayamıyorsa, gereken ek donanım/yazılım ve lisanslar teklife dahil edilmelidir.

5.2.25 Cihazlarda, syslog desteği bulunacaktır. Trafiğin log amaçlı uzak birden fazla syslog sunucusuna iletimi mümkün olmalıdır. Aynı zamanda syslog sunucu pool tanımlanarak logların gönderimi sırasında log sunucularından birisinin devre dışı kalması durumunda kesintisiz uzak sisteme loglamaya devam edebilmelidir.

5.2.26 Teklif edilecek ürün Gartner raporlarında lider kategorisinde yer almalıdır.

5.2.27 **Cihazın Yük Dengeleyici Özellikleri**

5.2.28 Cihazın throughput değeri en az 10 Gbps olacaktır.

5.2.29 Cihaz, HTTP trafiği için GZIP ve DEFLATE compression yapabilme özelliğine sahip olmalıdır.

5.2.30 Cihazlar 2.5 Gbps compression throughput sağlayacak şekilde lisanslanmalıdır. İleride donanım değişikliğine gerek olmadan lisans ile 5 Gbps'a yükseltilebilmelidir.

5.2.31 Cihaz üzerinde anlık olarak en az 10 Milyon eş zamanlı TCP session tutabilme kapasitesine sahip olmalıdır.

5.2.32 Yük dengelemeyle beraber sistem üzerinde SSL sonlandırma özelliği olacaktır. SSL Decryption (SSL şifresini çözme), cihaz üzerinde yapılıp, istemci - sistem arası HTTPS, sistem - sunucu arası, HTTP protokolü ile konuşacak şekilde konfigüre edilebilmeli ve farklı profiller tanımlanabilmelidir.

5.2.33 Sistemin kendi üzerinden, harici bir sisteme veri çıkmaya gerek kalmadan trafik akış takibi (flow tracking) yapılabilmelidir. Bunu sağlayacak yazılımlar (tcpdump vb.) sistem üzerinde yüklü olmalıdır.

5.2.34 Sistemin IPV6 desteği olacaktır. Bu özellik için lisans gerekiyorsa teklife dahil edilmelidir.

5.2.35 Değerleri ayarlanabilir sunucu durum takip, izleme (monitoring) ara yüzü bulunmalıdır. Timeout (zaman aşım süresi) ve interval değerleri tanımlanabilme özelliği olmalıdır.

5.2.36 Sunuculara veya sunucu guruplarına ayrı ve birden fazla izleme tanımı yapılabilmelidir.

5.2.37 Sunucuların izlenmesi ICMP, TCP, HTTP, HTTPS, FTP gibi protokolleri kullanarak yapılabilmelidir.

5.2.38 RTSP (Real Time Streaming Protocol) desteği bulunmalıdır.

5.2.39 Round Robin, Ratio, Fastest, Least Connection yük dengeleme algoritmalarına sahip olacaktır. Aynı zamanda, en hızlı cevap veren ve en az bağlantısı olan sunucuya istemcinin yönlendirilmesi sağlamalıdır.

5.2.40 Sistem, bütün sunucuların devre dışı kalması veya aktif üyelik bilgilerine bakarak yönlendirme (redirection) yapmalıdır.

5.2.41 Sistem, tüm HTTP isteklerini veya belli bağlantıları, otomatik olarak HTTPS 'e çevirebilme özelliği olacaktır.

5.2.42 İstemcinin sürekli aynı sunucuya bağlanmasını sağlayan Cookie persistence, Destination address affinity, hash persistence, SIP persistence, source address persistence, SSL persistence özelliklerini desteklemelidir.

5.2.43 Sistem, TCP ve UDP temelli bütün uygulamaları yük dengeli şekilde çalışacak ve akıllı yük dengelemesi yapabilmelidir.

5.2.44 L4 ve L7 özelliklerine göre trafiği yönetebilme özelliği olmalıdır.

5.2.45 Sistemin, L2 mode switching (anahtarlama), L3 mode routing (yönlendirme) özelliği olmalıdır.

5.2.46 HTTP isteğindeki herhangi bir bilgiye göre (URL, Domain, Cookie, IP gibi) anahtarlama (Content Switching) yapacaktır. Bağlantıdaki herhangi bir bilgiye bakarak, sunucu kümelerinde yük dengeleme yapmalıdır.

5.2.47 Sistem, DMZ ve intranetteki farklı alt ağlarda (subnet) bulunan sunucular için yük dengelemesi yapabilecek şekilde konumlandırılabilmelidir. DMZ ile lokal ağlar arasında, ağ seviyesinde izolasyon sağlayabilmelidir.

5.2.48 Sistemin 802.3ad link aggregation (bağlantı arabirimi birleştirme) desteklemelidir. Bu özellik için lisans gerekiyorsa teklife dahil edilmelidir Cihazlarda, Packet Filtering ve Access Control List özellikleri bulunacaktır. Cihazlar, cihaza giren ve cihazdan çıkan trafiği, IP adresi ve port seviyesinde kontrol edebilmelidir.

5.2.49 Sistem, Network Address/Port Translation yapabilmelidir.

5.2.50 Sistemin her ethernet portunda "VLAN" ve "Tagged VLAN" teknolojileri desteklemelidir.

5.2.51 Cihazlarda, scriptlerle sunucunun sağlık kontrolü (Health Check) yapılabilmeli, up/down anlama süresi ayarlama özelliği olacaktır.

5.2.52 Cihazların konfigürasyon yedeği, cihazdan harici ortama export (yedekleme) ve import (geri yükleme) özelliği olacaktır

5.2.53 Yük paylaşımı yapılan sunucuların günlük kayıtlarında, kullanıcıların IP adreslerinin görülmesini ve loglanmasını mümkün kılmalıdır.

5.2.54 Yük paylaşımı yapılan sunuculara yapılan istek loglarını cihaz üzerinden alınabilmelidir. Böylelikle Arka tarafta Load balance yapılan sunucularda log toplama ve korelasyon işleri tek noktadan yapılabilmesi sağlanmalıdır.

5.2.55 Yüklenici, harici bir gözlemleme sisteminin cihazlardan bilgi alabilmesi için gerekli XML API'leri sağlayacaktır.

5.2.56 Cihazın işletim sistemi, IP uygulama trafiğini giriş ve çıkış yönünde yakalamak, kesmek, dönüştürmek ve doğrudan yönlendirmek amacıyla kullanıcı tarafından kod yazılabilecek şekilde programlamayı destekleyecektir.

5.2.57 Sistemin Jumbo Frame desteği olmalıdır.

5.2.58 Sistem Spanning Tree Protokolünü (STP) desteklemelidir.

5.2.59 Sistemin 802.1p desteği olmalıdır. QoS için, diğer çevre ağ bileşenleri (switch, router vb.) tarafından set edilen 802.1p önceliklendirme taglarını anlayabilmeli ve uyumlu çalışmalıdır.

5.2.60 Sistem ağ sanallaştırma tünellerini (network virtualization tunnels) desteklemeli ve hem merkezi (centralized) hem de dağıtık (de-centralized) mimarilerde çalışabilmelidir.

5.2.61 Sistem VXLAN (Multicast), VXLAN (Unicast), NVGRE, Transparent Ethernet Bridging ağ sanallaştırmal tünel tiplerini desteklemelidir.

5.2.62 Sistem VXLAN ve non-VXLAN ağları arasında köprü vazifesi görebilmelidir (VLAN – VXLAN bridge)

5.2.63 Sistem üzerinden geçen trafik için, statik ve dinamik bantgenişliği kontrol politikaları (bandwidth control) tanımlamaya imkan sağlamalıdır. Tek bir bağlantı için eş zamanlı birden fazla farklı bantgenişliği politikası uygulanabilmelidir. Dinamik politikalar ile kaynak IP adresi dışında, kullanıcı ve bağlantı özelinde belirlenecek parametrelere göre (erişilen URL, kullanıcıya özel cookie, belirlenecek HTTP Header parametresi vb.) bantgenişliği kontrolü yapılabilmelidir.

5.2.64 Bantgenişliği kontrol politikaları sistem geneli için tanımlanabileceği gibi sanal sunucu (virtual server), paket filtrelerindeki bir kural (access list rule) veya traffic group/route domain özelinde de uygulanabilmelidir. Bu sayede bir kullanıcı veya bağlantının tüm sanal sunucu veya bir servisin bantgenişliği kaynaklarını tüketmesi engelllenebilmelidir.

5.2.65 Sistem ICSA sertifikalı ve “stateful” ağ güvenlik duvarı olarak çalışabilmelidir. Bu güvenlik duvarı ile Network DoS saldırıları tespit edilebilmeli ve önleyebilmelidir. Virtual Server, VLAN veya global bağlamda kaynak IP, hedef IP, protokol, kaynak port ve hedef port belirterek güvenlik kuralları yazılabilmelidir.

5.3 WEB UYGULAMA GÜVENLİK CİHAZI (2 Adet)

5.3.1 Uygulama Güvenlik Duvarı PCI DSS, HIPAA, Basel II, ve SOX standartlarına uygun olmalıdır.

5.3.2 Uygulama Güvenlik Duvarı ICSA güvenlik sertifikasına sahip olmalıdır.

5.3.3 Uygulama Güvenlik Duvarı, Policy-Based (“Positive”) security ve Signature-based (“Negative”) security özelliklerini desteklemeli, imza güncellemesi manuel ya da otomatik yapılabilmelidir. Yeni imzalar için evreleme özelliği olmalıdır. Buna ek olarak elle imza ya da regular expression olarak saldırı paternleri tanımlanabilir olmalıdır.

5.3.4 Teklif edilecek olan web uygulama güvenlik cihazı proje kapsamında yer alan yük dengeleme cihazı ile aynı donanımı kullanabilir olması tercih sebebidir.

5.3.5 Teklif edilecek olan web uygulama güvenlik cihazı 1 yıl boyunca cluster mimaride her iki fiziksel web uygulama güvenlik cihazı için 1 yıllık üretici destek paketi içerecektir.

5.3.6 Uygulama Güvenlik Duvarı, HTTP trafiğinin dışında SMTP ve FTP servisleri için güvenlik kuralları oluşturabilmelidir. FTP servisi için protokol, bruteforce ataklara karşı koruyabilmeli, FTP komutları için white list oluşturabilmeli. Komut uzunluklarını limitleyebilmeli SMTP servisi için greylist oluşturup spam atağına karşı koruyabilmeli, SMTP komutlarının kontrolü için black list oluşturabilmeli directory harvesting atakları azaltmalıdır.

5.3.7 Uygulama Güvenlik Duvarı, Layer 7 DoS, Brute Force, Cross-site scripting, Cross Site Request Forgery, SQL injection, Parameter tampering, Sensitive information leakage, Session high-jacking, Buffer overflows, Cookie manipulation, encoding attacks, Broken access control, Forceful browsing, Hidden fields manipulation, Request smuggling, XML bombs/DoS ataklarına karşı koruma sağlayabilmelidir.

5.3.8 Uygulama Güvenlik Duvarı, pozitif yaklaşım ile korudukları web sunucuların çalışma mantığını sayfalarda girilen input değerlerinin ne olması gerektiğini öğrenebilmeli ve bunlar haricindeki erişimlere izin vermemelidir. Gerektiğinde bu değerler elle müdahele edilerek değiştirilebilmelidir. Öğrenilen sayfaların değişmesi durumunda tekrar öğrenilmesi mümkün olmalıdır.

5.3.9 Uygulama Güvenlik Duvarı, realtime dinamik olarak policy oluşturabilmeli, otomatik self-learning ve policy oluşturma özelliğine sahip olmalıdır. Bu sayede zaafiyetleri keşfetme ve hızlı kurulum özelliklerine sahip olmalıdır. Çift yönlü çalışıp data ve protocol seviyesinde güvenlik sağlamalıdır.

5.3.10 Uygulama Güvenlik Duvarı, uygulamayı öğrenebilme üzelliğine sahip olmalıdır.

5.3.11 Uygulama Güvenlik Duvarı, Kredi Kartı ve vatandaşlık numarası gibi hassas dataları algılayabilmeli ve belirli politikalar takibinde bu bilgilerin anons edilmesini önleyebilmelidir.

5.3.12 Uygulama Güvenlik Duvarı, uygulamadan dönen hata kodlarını ve hata sayflarının görüntülenmesini engellemelidir.

5.3.13 Uygulama Güvenlik Duvarı, engellenen bir erişime ait kayıtları detaylı bir şekilde saklamalıdır. Bu kayıt en az tarih, saat, kaynak IP, hedef IP, hedef URL ve engelleme sebebi bilgilerini içermelidir.

5.3.14 Uygulama Güvenlik Duvarı, istenildiği takdirde üzerinden geçen HTTP isteklerini ve yanıtlarını ayrıntılı olarak loglayabilmelidir. Her bir istek veya yanıta bağımsız ve ayrı ID'ler atayarak takip kolaylığı sağlamalıdır.

5.3.15 Uygulama Güvenlik Duvarı, SSL içinden gelen saldırıları yakalayabilmelidir. Cihazın kendi üzerinde içerik filtreleme yapabilmesi tercih nedenidir.Yazılımcı tarafından unutulan klasörler, yedek dosyalar ve istemci tarafında istenmeyen HTTP isteği reddedilebilmelidir.

5.3.16 Uygulama Güvenlik Duvarı ile ilgili admin yetkileri sadece belli bir user rolunde olmalıdır.

5.3.17 Uygulama Güvenlik Duvarı, üzerinde ayrıntılı rapor alınabilmelidir. Application Firewall'a yönelik raporlar, audit raporları alınabilmesi tercih nedenidir, rapor formatı PDF olmalıdır. Raporlar Schedule edilebilmelidir. Email ile göderilebilmelidir.

5.3.18 Uygulama Güvenlik Duvarı, XML firewall özelliği olmalı, aşağıdaki fonksiyonlara sahip olmalıdır: WSDL Method Filtering, XML content inspection/validation, XML Denial of Service (XdoS) Recursive Expansion Attack, SQL injection via XML (Xpath) prevention, XML attachment security SOAP message validation, Schema validation, Request rate limiting

5.3.19 Uygulama Güvenlik Duvarı, üçüncü parti uygulama ve cihazlarla entegere olarak çalışabilmelidir, örneğin Splunk, WhiteHat, ve ArcSight.

5.3.20 Uygulama Güvenlik Duvarının Web Scraping koruma özelliği olmalıdır; Rate limiting, heuristics ve algorithms özellikleri ile uygulama hakkında bilgi alanın botnet olup olmadığını ayırt edebilmelidir.

5.3.21 Uygulama Güvenlik Duvarı kullanıcının doğrulanması ve sunucu gecikmelerini inceleyerek Dos/DDoS ataklarını anlayabilmelidir.

5.3.22 Uygulama Güvenlik Duvarı, güvenlik kurallarını XML formatında export ederek audit ve off-line olarak programatik değişiklik için kullanabilme özelliğine sahip olmalıdır.

5.4 YETKİLİ HESAP ŞİFRE YÖNETİMİ VE OTURUM İZLEME YAZILIMI (1 Yazılım 10 Kullanıcı)

5.4.1 Genel Platform Koşulları

5.4.2 YHŞGİS, İdarenin altyapısında kullanılan sunucuları yöneten en az 10 sistem yöneticisinin şifreleri yönetebilmesi için Yetkili Şifre Yönetimi yazılımı Yetkili Oturum Yönetimi / Aktivite İzlemesi yapacaktır.

5.4.3 YHŞGİS yazılımının felaket kurtarma desteği ve ilgili modülleri ile birlikte olacaktır.

5.4.4 Sunucu ve istemci makinalarda, yerel yönetici hesaplarını yönetecektir.

5.4.5 Yönetilecek olan hesaplarda herhangi bir kısıtlama ve/veya sınırlama olmayacaktır.

5.4.6 Yönetilecek hesaplar sisteme toplu olarak girilebilecektir

5.4.7 Kullanılacak çözüm, VMware, Microsoft Active Directory, Unix/Linux tabanlı sistemleri otomatik veya belirtilen zamanda tarayarak, buralarda bulunan yetkili hesapları sistem içerisine dâhil edecektir.

5.4.8 Bu otomatik bulma işlemi sırasında tespit edilen hesaplar, Servis, Zamana bağlı görev vb. içerisinde bulunuyorsa bu bilgiler de otomatik olarak tanımlanabilecektir. Yeni eklenen veya çıkartılan sistemler algılanabilecektir. Yeni eklenen veya çıkartılan sistemlere otomatik kurallar uygulanabilecektir.

5.4.9 Farklı hesaplara farklı politikalar uygulanabilecektir.

5.4.10 Hesaplara ait şifrelerin doğruluğu düzenli olarak kontrol edilebilecek ve raporlanabilecektir.

5.4.11 Hesaplar esnek şekilde gruplanabilecektir.

5.4.12 YHŞGİS, İdarenin ihtiyacı olan sınırsız sayıda şifreyi saklayacaktır.

5.4.13 YHŞGİS, tek bir arayüz ile merkezi olarak yönetilecektir.

5.4.14 YHŞGİS, Yönetim ve Kullanıcı Arayüzü web tabanlı olacaktır.

5.4.15 YHŞGİS arka planda bir veritabanı kullanılıyorsa, bu veritabanı ürün tarafından otomatik olarak yönetilebilecektir.

5.4.16 YHŞGİS, her bir Sistem Yöneticisinin sadece kendi yönettiği sistemlerdeki hesapları ve şifreleri görebilmelerine, imkân sağlayacaktır.

5.4.17 Sistem Yöneticilerinin sistemi kullanan kişilere ait hesapları ve şifreleri görebilmeleri engellenecektir.

5.4.18 Microsoft Active Directory ya da LDAP tabanlı herhangi bir dizin ile entegre edilebilecektir. Aynı şekilde bu dizinlerde bulunan kullanıcı grupları sayesinde otomatik yetkilendirmeler yapılabilecektir.

5.4.19 İstendiğinde hesaplarda toplu olarak işlem yapılabilecektir.

5.4.20 Kullanıcılara zaman, kaynak IP adresi gibi erişim kısıtlamaları uygulanabilecektir.

5.4.21 VM desteği olacaktır. Yazılım sanal sunucu üzerinde çalışan işletim sistemlerine kurulabilecektir. Bu sayede sunucu sistem donanımı İdarenin ihtiyacına göre değiştirilebilecektir.

5.4.22 Önerilen çözüm İdare ihtiyaçlarının artması doğrultusunda lisans artırımı ile genişleyebilecek özellikte olacaktır.

5.4.23 Ürünün Felaket Kurtarma (DR) ve Süreklilik (HA) desteği olacaktır.

5.4.24 Farklı Segmentlerdeki dağınık yapılar, tek bir merkezden yönetilebilecektir.

5.4.25

5.4.26 Ürünün API desteği olmalıdır.

5.4.27 Teklif edilen üründe kullanılan şifreleme algoritmaları FIPS 140-2 uyumlu olacaktır.

5.4.28 Tüm Sistem bileşenleri kendi aralarındaki iletişimi kriptolu olarak yapacaktır.

5.4.29 Ürünün yedekleri kriptolu olarak tutulacaktır.

5.4.30 Şifrelerin saklandığı yer izole “Güvenli Bölge” olacaktır.

5.4.31 Şifrelerin saklandığı sistemi yöneten kişilerin, saklanan şifrelere erişimi olmayacaktır.

5.4.32 Video kayıtları, loglar, kurallar vb. şifreli ve güvenli şekilde saklanacaktır.

5.4.33 Ürüne olan girişler iki-adımlı doğrulama sistemleri ile entegre olabilecektir. (two-factor authentication)

5.4.34 Çözüm üzerinde otomatik yedekleme özellikleri olacaktır, alınan yedeklerin yine otomatik olarak bir arşiv sunucusuna alınacaktır.

5.4.35 LDAP, Windows SSO, PKI, RADIUS gibi Kimlik Doğrulama Yöntem'leri ile uyumlu olacaktır.

5.4.36 Büyük yapıdaki LDAP/AD içerisinde çok yönlü sorgulama ve kontrol yapılabilecektir.

5.4.37 Şifre objesine erişim için çağrı açma ve yetkilendirme sistemi olacaktır.

5.4.38 SIEM ürünleri ile entegrasyonu olacaktır.

5.4.39 Kimlik Yönetimi Sistemleri ile entegrasyonu olacaktır.

5.4.40 Zafiyet Yönetimi (Vulnerability Management) ürünleri ile entegrasyonu olacaktır.

5.4.41 Raporların, istenilen zamanlarda ya da belirli aralıklarla alınabilmesi mümkün olmalıdır.

5.4.42 Tüm yöneticilerin hareketleri raporlanabilecektir.

5.4.43 Rapor çıktıları en az Excel veya CSV formatlarını destekleyecektir.

5.4.44 Sisteme girişlerin hareketleri raporlanabilecektir.

5.4.45 Şifrelerin, kullanıcılar tarafından istendiği ve bırakıldığı bilgisi raporlanabilecektir.

5.4.46 Değiştirilemeyen şifreler raporlanabilecektir.

5.4.47 Doğrulanamayan şifreler raporlanabilecektir.

5.4.48 Değiştirilen şifreler raporlanabilecektir.

5.4.49 Uzlaştırıcı hesap hareketleri raporlanabilecektir. (şayet bir kullanıcı şifresi uyuşmazlık gösterirse, bir başka üst yetkili kullanıcı ile diğer problemli kullanıcının şifresi otomatik/manuel değiştirilecektir)

5.4.50 Sistem ID veya aygıt türüne göre raporlanabilecektir.

5.4.51 Şifrelerin durumları raporlanabilecektir.

5.4.52 Raporlar kişiselleştirilebilecek ya da önceden şablon olarak oluşturulabilecektir.

5.4.53 Data Export Edilebilecektir.

5.4.54 Raporları görecek kişiler kısıtlanabilecektir.

5.4.55 Adli İncelemeler için Video Kayıtları tekrar izlenebilecektir.

5.4.56 Video kayıtları herhangi bir bilgisayarda izlenebilmek üzere kaydedilebilecektir.

5.4.57 Belirlenen kullanıcıların onay mekanizmasına ihtiyaç duymadan yetkili hesaplara erişimi mümkün olabilecektir.

5.4.58 İş akışları izlenebilecek ve raporlanabilecektir.

5.4.59

5.4.60 Şifre Yönetimi ve Yetkili Hesap Yönetimi

5.4.61 Yazılım belirli zaman aralıklarında şifreleri otomatik olarak değiştirecektir.

5.4.62 ifreler tek kullanımlık olabilecektir. Grup, Platform ya da Sistem bazında uygulanabilecektir.

5.4.63 Şifreler manuel olarak, politikaya bağlı olarak ya da doğrulama hatasından sonra otomatik olarak değişebilecektir.

5.4.64 Hesaplara rastgele şifre atanabilecektir. Aşağıda belirtilen durumlarda şifreler atanabilecektir:

5.4.65 Hesap Yöneticisi tarafından istenildiğinde,

5.4.66 Politikaya bağlı olarak zamanı geldiğinde,

5.4.67 Kullanım süresi bittiğinde atanabilecektir.

5.4.68 Şifreler otomatik olarak hedef sistem üzerinde doğrulanabilecektir.

5.4.69 Şifreler periyodik olarak kontrol edilip, doğrulanamayan şifreler otomatik olarak uyarı verecektir.

5.4.70 Doğrulanamayan şifreler raporlanacaktır.

5.4.71 Atanacak şifrelerin uzunluk, karmaşıklık vb. özelliklerin tüm hedef cihazlar için belirlenebilecektir.

5.4.72 Şifrelerin geri dönük sürümlerinin, sistemde tutulması ve gerektiğinde bunlara erişilmesi mümkün olacaktır.

5.4.73 Otomatik şifre değiştirme işlemlerinde kullanılan şifre politikalarını, manuel değiştirme yaparken de kullanabilecektir.

5.4.74 Şifre değiştirme işlemi yapılırken, daha önceden kullanılmış şifrelerin tekrar kullanılmasını engelleyecektir.

5.4.75 Her hedef cihaz için farklı şifre üretebilecektir.

5.4.76 Hedef cihaz tipleri aynı olsa bile, farklı politikalar uygulayabilecektir.

5.4.77 Şifre yönetimi ve oturum kayıt işlemleri için birleşik politika uygulayabilecektir.

5.4.78 AD ve LDAP çoklu desteği olacaktır.

5.4.79 Tek kullanımlık şifre oluşturma mümkün olacaktır.

5.4.80 Aktiviteler hakkında mail ile uyarı iletebilecektir.

5.4.81 Şifre kilitleme işlemi yapılabilecektir. Bir kullanıcı şifreye eriştiğinde, diğer kullanıcıların o şifreye erişmesi engellenebilecektir.

5.4.82 Aynı şifreyi bekleyen kullanıcıya, şifrenin artık kullanılabilir olduğu bilgisi gidecektir.

5.4.83 Ürün; şifrenin süresinin biteceği bilgisi zamanı gelmeden önce kullanıcıya e-posta ile bildirecektir.

5.4.84 Aynı hesabın şifresinin, birden fazla kullanıcının aynı anda kullanmasını engelleyecektir.

5.4.85 Hedef sisteme bağlantı yapılabilecek, şifre görme ya da yazma ihtiyacı olmadan bağlanabilecektir.

5.4.86 Windows tabanlı hedef cihazlara, ürün üzerinden direk bağlantı yapabilecektir.

5.4.87 Unix/Linux tabanlı hedef cihazlara, ürün üzerinden SSH ile direkt bağlantı yapabilecektir.

5.4.88 Mevcutta desteklenen cihazların dışındaki hedef sistemler için, dinamik destek sağlanabilecektir.

5.4.89 Hedef Sistem Erişimi - Değişikliği - Şifre Kullanımı - Şifre Kullanım isteği ile ilgili e-posta atabilecektir.

5.4.90 Dosya içerisindeki text tabanlı şifrelerin toplanması ve güncellenmesine dair olanaklar açıklanacaktır.

5.4.91 Ortak kullanılan şifreler için check-in check-out sistemi olup olmadığı belirtilecektir.

5.4.92 Bir grup sistem için aynı şifreyi üretme olanağına sahip olacaktır.

5.4.93 Yetkili Aktivite İzleme / Video Kaydı

5.4.94 İdare içerisinde ağ yalıtımı, hedef sunuculara güvenli erişim, oturum aktivitelerinin kayıt edilmesi ve uygulama kullanıcıların şifre bilgilerini görmeden hedef sistemlere ait uygulamaları çalışabilmesidir. Bunu sağlayacak sistem aşağıdaki maddelerde tanımlanan özelliklere sahip olacaktır.

5.4.95 Ürün, hedef kaynaktaki oturumların kontrol edilebilmesi için mevcut ağ yapısının değiştirilmesine ihtiyaç duymayacaktır.

5.4.96 Denetim personeli, yetkilerine göre tüm kayıtlara erişebilecek ve izleyebilecektir.

5.4.97 Kayıtlar, şifreli bir şekilde güvenli bir alanda saklanacaktır.

5.4.98 İstenildiğinde, kullanıcıya Şifre Objesini göstermeden, güvenli uzak bağlantı kurabilmesi sağlanacaktır.

5.4.99 İstenildiğinde, hedef sunuculara sadece ürün üzerinde bağlantı yapması sağlanabilecektir.

5.4.100 Hesapların yönetilmesi, oturumların kontrolü ve izlenmesi tek bir arabirimden yapılabilecektir.

5.4.101 Ürün, herhangi kişinin sistemle bağlantı kurduğunda, yaptığı işlemlerin sadece o kişinin sorumluluğunda olduğunu gösterebilecek denetim altyapısını sağlayacaktır.

5.4.102 İstenildiğinde belirli kullanıcı veya gruplar için aktivite kaydı devre dışı bırakılabilecektir.

5.4.103 Video kaydı dışında belirli protokoller için metin tabanlı kayıtlar da bulunacaktır. Bu kayıtlar içerisinde arama yapılabilecektir.

5.4.104 Video kayıtlarında, kullanılan komutlar arasında arama yapılabilecektir. (Unix, veritabanı vb. çalıştırılan komutlar ve sorgular)

5.4.105 Ağ yalıtımı sağlama amacıyla güvenli Proxy olarak çalışabilecektir.

5.4.106 Çağrı açma, yardım masası, değişiklik yönetimi gibi sistemler ile entegre olabilecektir. Bu sayede oturum açılmadan önce onay mekanizması getirilebilecektir.

5.4.107 Oturumlar, kayıt esnasında gerçek zamanlı olarak seyredilebilecektir.

5.4.108 Oturumlar, kayıt esnasında yönetici tarafından sonlandırılabilecektir.

5.4.109 Kayıtlar renkli olarak ve orijinal çözünürlükte kaydedilebilecektir.

5.4.110 Çoklu domain desteği olacaktır.

5.4.111 Yüksek erişilebilirlik için yedekli yapıyı destekleyecektir.

5.4.112 Unix tarafında komut belirleme (Whitelisting) özellikleri bulunacaktır.

5.4.113 AD bridge özelliği sunacaktır.

5.4.114 Oturum yönetimi ve kaydı tüm protokolleri kapsayacaktır.

5.4.115 Kullanıcılar uzak windows sistemlere herhangi bir RDP istemci kullanarak direkt bağlanabilecektir.

5.4.116 Kullanıcılar kayıt edilmiş RDP dosyalarını Session recording için kullanabilecektir.

5.4.117 Kullanıcılar, uzak sistemlere native olarak tüm SSH clientlardan bağlanabilecektir.

5.4.118 Uzak sistemlere yapılan SSH bağlantıları için client veya server tarafında agent yüklenmeden komutları belirleme işlemi (whitelisting) yapabilecektir.

5.4.119 SSH recording backspaces, arrows, tabs, command history gibi atlatma yöntemlerini engellemeyi destekleyecektir.

5.4.120 Native SSH recording sırasında RADIUS authentication desteği olacaktır.

5.4.121 SSH destekli her türlü cihazın entegrasyonu yapılacaktır.

6 Diğer Konular

6.1 Tanımlar

6.1.1 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.

6.2 Proje Esnasındaki SLA Seviyeleri ve Diğer Hizmet Parametreleri

6.2.1 Aşağıda, projenin teslimine kadar olan sürede uygulanacak SLA'ler belirtilmiştir.

6.2.2 Yüklenici, aşağıdaki SLA'lere uygun bir arıza/destek sistemi ve sürecini Kurum'un hizmetine projenin başlangıcında sunmalıdır.

6.2.3 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

6.3 Yemek ve Ulaşım

6.3.1 Danışmanlara öğle yemeği, Üsküdar Üniversitesi tarafından sağlanacaktır.

6.3.2 Danışmanların ulaşım hizmeti Üsküdar Üniversitesi tarafından sağlanmayacaktır. Yüklenicinin bununla ilgili lojistik planlamayı yapması gerekmektedir.

6.4 Teklif için Para Birimi

6.4.1.1 Hizmet için verilen teklifler Türk Lirası cinsinden verilmelidir.

7 Finansal Bilgiler

8.1 Sözleşme Konuları

8.2 Teminatlar, Teklif Şekli, Kur Uygulaması, Vade ve Ödeme Şekli

8.3 Genel Hüküm ve Şartlar

7.1 Teklif, Zaman Tabloları ve Kabul Şartları

7.1.1 Zaman Tablosu

7.1.2 Aşağıdaki tarih tablosuna uygun olarak teklifler değerlendirilecektir. Bu tarihler, Üsküdar Üniversitesi iş yoğunluğu, beklentileri doğrultusunda değiştirilebilir.

7.1.3 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	

7.2 Firma Tarafından Doldurulacak Tablolar

7.2.1 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.

7.2.2 Üsküdar Üniversitesi, referans olarak gösterilen proje/firmaları ziyaret etmek isteyebilir. Teklif veren firma, Üsküdar Üniversitesinin istemesi durumunda bu firmalara ziyaret planlamakla yükümlüdür.

7.2.3 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 :**	

7.3 Kabul Şartları

7.3.1 Proje, tüm bileşenleri ile bitirildiği zaman Kurum tarafından kabul işlemi yapılacaktır. Projenin kabulü yapılmadan bitmiş sayılmayacaktır. Kabul şartları aşağıdaki gibidir.

7.3.2 Teklifteki tüm cihazlar eksiksiz bir şekilde kurulmuş çalışıyor olmalı

7.3.3 Tüm sanal makineler yeni yapıya taşınmış olmalı

7.3.4 Tüm danışmanlıklar verilmiş olmalı

7.3.5 Tüm yedekleme ve iş sürekliliği sistemlerinde tam fonksiyonel testler yapılmış olmalı

7.3.6 Tüm sistemler, sorunsuz 30 gün boyunca çalışıyor olmalı

7.3.7 Tüm eğitimler verilmiş olmalı

7.3.8 Projeye ait tüm dokümanların Kurum'a teslim edilmiş olması