****

**SUNUCU ve VERİ DEPOLAMA SİSTEMLERİ**

**TEKNİK ŞARTNAMESİ**

**SUNUCU SİSTEMİ 1 ADET**

1.1. Sunucu GPU uyumlu olmalıdır.

1.2. AMD EPYC 7000 serisi işlemcilerinin takılabilmesine imkân tanıyan soket bulunmalıdır. En az 2 (iki) işlemci takılmasına uygun olmalıdır.

1.3. İşlemciler AMD EPYC 7702 2GHz 64-core çekirdekli veya dengi olmalıdır. İşlemci sayısı 2 (iki) adet olmalıdır.

1.4. İşlemciler üzerinde orijinal soğutucu bulunmalıdır.

1.5. Anakart üzerinde en az 32 adet DDR4 destekli bellek soketi bulunmalıdır.

1.6. Sunucu DDR4 RDIMM tip bellekleri desteklemelidir.

1.7. 1TB DDR4 3200 MT/s RDIMM (en az 64 GB parçalar şeklinde) kapasitede hafıza sunucu üzerine takılı olmalıdır.

1.8. Sistem belleği toplamda en az 4 TB ‘a kadar yükseltilebilmelidir.

1.9. Anakart üzerinde en az 5 (beş) adet tam(fiziksel olarak X16) boy PCIe 4.0 genişleme yuvası olmalıdır.

1.10. Anakart üzerinde uzaktan yönetim kartı bulunmalıdır. Bu arabirim, ekstra bir yönetim yazılım olmadan, birden fazla sistemin tek ekrandan yönetilmesine imkân tanımalıdır. Bu özellik için herhangi bir lisans gerekiyorsa teklife dâhil edilecektir.

1.11. Sunucu ön panelinde bulunan USB portlardan bir adeti uzaktan yönetim portu tarafından erişilebilmeli, sunucu kapalı olduğu esnada bu port üzerinden takılabilecek USB bellek ile firmware güncellemesi veya provizyonlama yapılabilmeli ve uzaktan yönetim networkünün kurulu olmadığı veya çalışmadığı esnada USB kablo ile bir bilgisayara bağlayarak uzaktan yönetim web ara yüzüne erişilebilmelidir

1.12. En az 16MB bellekli dâhili ekran kartı olmalıdır.

1.13. 19” Rack tipi olmalı ve rack de kapladığı alan en fazla 2U olmalıdır.

1.14. Üzerinde en az 8 (sekiz) adet 2.5” NVMe disk yuvası bulunmalıdır.

1.15. Kasa içinde yedekli, çalışırken takılıp-çıkarılabilir yüksek performanslı en az 6 adet fan bulunmalıdır.

1.15. En az 2 (iki) adet ve en az 2400 Watt gücünde güç kaynağı olmalıdır.

1.16. Güç kaynağı 200-240 V gerilim aralığında çalışabiliyor olmalıdır.

1.17. Sunucuda bulunan fan ve güç kaynakları yedekli özellikleri standart olmalıdır, sonradan eklenmiş olmamalıdır.

1.18. Sistemde en az 1 (bir) adet donanımsal RAID denetleyici olmalı ve PCI-e yolu üzerinde çalışmalıdır. RAID denetleyicisi RAID 0, 1, 10, 5, 50, 60 seviyelerini desteklemelidir.

1.20. RAID denetleyici en az 8 GB ön belleğe sahip olmalıdır.

1.21. RAID denetleyici en az 16 adet mantıksal birim oluşturmaya imkân vermelidir.

1.22. Çevrimiçi olarak RAID Seviyeleri değişebilmeli ve kapasite artırımı yapılabilmelidir.

1.23. Sunucuda en az 3 adet 15.36TB NVMe disk takılı olmalıdır.

1.24. Sabit Disk yuvaları çalışırken takılabilir olmalıdır.

1.25. Microsoft Windows Server 2016, 2019, Ubuntu LTS ve VMware Sanallaştırma yazılımlarını (güncel kararlı sürümleri) ve işletim sistemlerini desteklemelidir.

1.26. Sunucu üzerinde network bağlantısı için en az 4 adet 10 Gbps (10GBASE-T) destekli bağlantı noktası mevcut olmalıdır.

1.27. En az 3 adet USB 2.0 (veya üzeri) yuvası olmalıdır.

1.28. Teklif edilecek sunucunun Bluetooth Low Energy (BLE) veya wireless teknolojisi kullanarak cep telefonu veya tablet üzerinden erişim ve yönetim desteği olmalıdır.

1.29. Sunucu üzerinde takılan bellek modüllerinin uyumlu olup olmadığını algılayabilmeli ve raporlayabilmelidir.

1.30. 19” rack kabinete takmak için gerekli ek parçalar ile teklif edilmelidir.

1.31. Sunucular ürün üreticisi tarafından sağlanan 3 yıl yerinde parça değişimini içeren destek paketi (en geç ertesi gün müdahale) ile teklif edilmelidir.

**VERİ DEPOLAMA 1 ADET**

* 1. Teklif edilecek 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. Teklif edilen veri depolama ünitesi, 32Gb FC, 25Gb ISCSI, 10 Gb Base-T ISCSI ve 12 Gb SAS portları ile sunucu bağlantısını sağlayabilmelidir. Teklif edilen veri depolama ünitesi üzerine ihtiyaca göre en az 8 adet 32 Gb FC, 25 Gb ISCSI, 10 Gb Base-T ISCSI ve 12 Gb SAS portları takılabilmelidir.
  3. Teklif edilen veri depolama ünitesi SAN ve DAS formatlarını desteklemelidir. Teklif edilen veri depolama sistemi SAN formatında teklif edilecektir.
  4. Harici depolama sistemi üzerinde iki adet kontrol ünitesi (dual controller) bulunmalıdır.
  5. Her kontrol ünitesi (controller) üzerinde 32 Gbps hızında en az 4 (dört) adet FC port olmak üzere toplamda en az 8 adet 32 Gbps hızında FC port bulunacaktır.
  6. Teklif edilecek harici depolama sistemi sunucu sistemlere FC ara yüzü ile bağlanmalıdır.
  7. Depolama ünitesi ile birlikte en az 8 (sekiz) adet 16GB Fiber SFP optik modül verilecektir. Tüm kitler depolama üreticisine ait olmalıdır.
  8. Her kontrol ünitesi yönetim için en az 1Gbps hızına sahip yönetim portu bulunmalıdır.
  9. Teklif edilecek harici disk ünitesi üzerinde bulunan her kontrol ünitesi üzerinde en az 16 (Onaltı) GB toplamda ise 32(otuziki) GB bellek bulunmalıdır.
  10. Teklif edilen veri depolama ünitelerinin backplane hızı en az 12Gbps olmalıdır.
  11. Çalışan sistem üzerinde kesinti yaratmadan firmware güncellemeleri yapılabilmelidir.
  12. Depolama Ünitesi, teklif edilen kontrol birimleri ile en az 276 adet disk kapasitesine genişleyebilmeli ve en az 4PB kapasitesine kadar büyüyebilmelidir.
  13. Sistem disk artırımı raflar şeklinde arttırılabilir olmalı ve bu raflar entegre bir HTML5 web tabanlı GUI arayüzü ile yönetilebilir olmalıdır. Raflar toplam disk sayısını sağlamak üzere 12 (oniki) adet 3.5” veya 24 (yirmidört) adet 2.5” disklerden oluşturulabilmeli ve raflar arasındaki bağlantı 12 Gbit hızında SAS arayüz ile yapılmalıdır. Rafların her biri en fazla 2U yükseklikte olmalıdır. Bunların haricinde diskler istendiğinde 84 disk alabilen 5U yüksekliğinde 2.5” ve 3.5” karışık kullanılabilen disk çekmeceleri/kontrol ünitesi ile de tekliflendirme yapılabilir olmalıdır.
  14. Sistem üzerinde en az 17 adet 3.84 TB SAS SSD ve 24 adet 12 TB NLSAS disk bulunmalıdır..
  15. Kullanılan diskler seçilen disk raflarına uygun şekilde yüksek performanslı SAS, NL-SAS, SSD ve FIPS sertifikalı self-encrypting SAS,NLSAS ve SSD olabilmelidir.
  16. Teklif edilen veri depolama sistemi her disk in yaptığı I/O yu izlemeli sağlık durumunu performans grafiğini proaktif olarak izlemeli ve disk bozulmadan önce gerekli uyarıları verecek şekilde çalışmalıdır. Bunu sağlayamayan sistemler %30 ilave kapasite verecek şekilde teklif etmelidirler.
  17. Sistem, üzerinde disk arızaları meydana geldiği zaman, yeniden oluşturma sürelerini azaltan Distributed RAID veya benzeri bir teknolojiye sahip olmalıdır.
  18. Sistem Fiber bağlantı seçeneği ile en az 256 adet host bağlantısını destekleyebilmelidir.
  19. Teklif edilen veri depolama ünitesi ile sunucunun FC olarak bağlantısı yapılamıyorsa her bir veri depolama ünitesi ile birlikte en az 24 portlu en az 16 portu aktif olarak çalışan 16Gb/s SAN switch teklife dahil edilmelidir. SAN switch için gerekli lisans ve SFP GBIC ler de teklife dahil edilmelidir.
  20. Harici disk sistemi 0, 1, 5, 6 ve 10 RAID seviyelerini desteklemelidir.
  21. Sistemde kullanılmakta olan sanal disk gruplarına erişim kesintisi olmadan ilaveler yapılabilmelidir.
  22. Teklif edilen veri depolama ünitesi ile ileri tarihlerde ek maliyet olmaması açısından tüm lisanslar (snapshot, clone, read cache, auto tiering, replikasyon vb.) birlikte verilmelidir.
  23. Teklif edilen sistem SSD lerin cache olarak kullanabilmesine izin vermelidir. Cache miktarı istenildiği takdirde 4TB’a kadar yükseltilebilmelidir.
  24. Teklif edilen veri depolama ünitesi otomatik katmanlandırma (auto-tiering) teknolojisini desteklemelidir.
  25. Teklif edilen veri depolama ünitesi “thin provisioning” desteği olmalıdır.
  26. Teklif edilen veri depolama ünitesinde her kontrol ünitesi (controller) başına en az 512 (beşyüzoniki) LUN yaratılabilmelidir.
  27. Teklif edilen veri depolama ünitesinin en az 1024 adet snapshot desteği olmalıdır.
  28. Teklif edilen veri depolama ünitesi yedekli güç kaynağına (redundant power supply) sahip olmalıdır. Veri depolama ünitesi ile birlikte 2 adet güç kablosu verilmelidir.
  29. Harici disk ünitesi en az Vmware 7.0 ve 6.7; Windows Server 2022, 2019 ve 2016, RHEL 8.2 ve 7.8, SLES 15.2 ve 12.5 işletim sistemlerini desteklemelidir.
  30. Harici disk ünitesinin VMware vSphere (ESXi), Microsoft Hyper-V ve vCenter SRM desteği olmalıdır.
  31. Veri Depolama sisteminin yönetimi ek bir yazılım yüklemeye gerek kalmadan web tabanlı olarak yapılabilmelidir.
  32. Veri depolama ünitesi en az 3 yıl boyunca ertesi iş günü üretici garantisine sahip olacaktır.

**NETWORK VERİ DEPOLAMA 1 ADET**

NAS Cihazı Teknik Özellikleri

1. Ağa (network) bağlanabilen veri depolama ünitesi (Network Attached Storage Server (NAS Server)) cihazı olacaktır.

2. Üzerinde en az 2 adet 10Gb ve 2 adet 1Gb Base-T ve en az 4 adet 16Gb FC portu bulunacaktır.

3. En fazla 2 (iki) U yüksekliğinde ve raf tipinde olacaktır. Kabin montaj kiti/aparatları cihazla birlikte verilecektir.

4. İşlemci kapasitesi en az 12-Core 2.2 (iki nokta iki) Ghz olacaktır ve 2 adet olacaktır.

5. Üzerinde en az 2 (iki) adet USB 3.0 portu olacaktır.

6. En az 64 (altmış dört) GB ECC özellikli memory olacaktır.

7. En az 12 (on iki) adet hot-plug disk yuvası bulunacaktır.

8. RAID 0, RAID 1, RAID 5, RAID 6 ve RAID 10 desteği olacaktır.

9. SMB 3.0, NFS, FTP, CIFS, SMB Direct (RDMA) dosya erişim protokollerini destekleyecektir.

10. Vmware vSphere, Microsoft Hyper-V destekli bağlantı sistemleriyle uyumlu çalışabilecektir.

11. Üzerinde en az 2 (iki) adet güç ünitesi olacak ve sökülüp takılabilir özellikte olacaklardır.

12. En az 4 (dört) adet en az 2 (iki) TB en az 7.2K rpm 3.5 inç 6Gb SATA disk ile birlikte verilecektir. Ham kapasitesi en az 8 (sekiz) TB olacaktır.

13. Cihaz ile beraber verilen diskler NAS üreticisinin web sitesindeki uygunluk listesinde yayınladığı disklerden olacaktır.

14. En az 3 yıl ertesi iş günü destek hizmeti olmalıdır.

**YEDEKLEME YAZILIMI 1 ADET**

1. Yedekleme yazılımının ana modülü 64-bit Windows 2012, 2016 ve 2019 işletim sistemleri üzerinde çalışabilmelidir.
2. Yedekleme yazılımı Windows (8, 10,11, 2012, 2016, 2019, 2022), Linux (Ubuntu, XenServer, Debian, Oracle Linux, Red Hat, SUSE, CentOS) ve Unix (IBM AIX, Sun Solaris) işletim sistemlerini ajan yardımıyla yedekleyebilmelidir.
3. Yedekleme yazılımı Exchange, MS SQL Veritabanı, Windows Active Directory, SharePoint, Oracle Veritabanı ve Enterprise Vault uygulamaları için ajan desteği içermelidir. Bu sayede söz konusu uygulamalar çevrimiçi olarak yedeklenebilecektir.
4. Yedekleme yazılımı, yapılan yedekleme işlemleri, kartuş yönetimi vb. ile ilgili kayıtları beraberinde sağladığı bir veritabanında tutabilmelidir. İlave bir veritabanı yazılımı kullanımına gerek duyulmamalıdır.
5. Yedekleme yazılımının kullandığı veritabanı için otomatik bir bakım işlemi takvimlenebilmelidir.
6. Yedekleme yazılımının yedeklediği veriye ilişkin katalog bilgisini kartuşa da yazmalıdır. Bu sayede gerektiği durumda kartuştaki bu bilgi geri dönüşler için kullanılabilmelidir.
7. Yedekleme yazılımı tam (full), arttırımlı (incremental) ve farklı (differential) yedekleme ve farklı medya türleri (disk, fiziksel teyp, sanal teyp) arasında imaj kopyalama (duplication) operasyonlarını yapabilmelidir.
8. Yedekleme yazılımı bir tam yedek ve ona bağlı arttırımsal yedeklerden yeni bir tam yedek seti yaratabilmelidir. Sürekli arttırımsal özelliği ile full yedeği kendi yönetebilmelidir.
9. Yedekleme yazılımı sağladığı filtreleme imkanı sayesinde istenmeyen dosyaların yedeklenmesini önleyebilmelidir.
10. Yedekleme yazılımı yedekleme işleminin başlangıç ve bitiş zamanlarını, toplam yedekleme hacmini ve yedeklemenin başarı durumunu yönetim konsolu vasıtasıyla sergileyecektir.
11. Yedekleme yazılımı yapmış olduğu yedekleme ve kurtarma işlemlerini tarih sırasına göre listeleyebilmelidir.
12. Yedekleme yazılımı açık dosyaların da yedeklenmesini sağlamalıdır. Bu özelliğin sağlanabilmesi için ek bir lisans maliyeti gerekmemelidir.
13. Yedekleme yazılımı yapılan yedekleme ve kurtarma işlemlerinde çıkabilecek sorunları raporlayacak ve sorun çıkması durumunda belirlenen yöneticiye e-posta ile anında otomatik olarak bildirme kabiliyetine sahip olmalıdır.
14. Yedekleme yazılımı gerçekleştirdiği yedekleme, kurtarma, konfigürasyon oluşturma/değiştirme ve raporlama operasyonlarını tek bir ara yüz ile izleme ve yönetme özelliği içermelidir.
15. Yedekleme yazılımı medya havuzlarını desteklemelidir.
16. Yedekleme yazılımı kullandığı yedekleme cihazında bulunan kartuşları barkod etiketi ile tanıma kabiliyeti olmalıdır.
17. Yedekleme yazılımı T10 olarak isimlendirilen teyp sürücü temelli veri şifrelemesi standardını desteklemelidir.
18. Yedekleme yazılımı yerel ve uzak NDMP desteği içermelidir.
19. Yedekleme yazılımı Oracle RAC (11G, 12C, 18C) veritabanının çevrimiçi yedeğini alabilmelidir.
20. Yedekleme yazılımı Microsoft Exchange 2013, Exchange 2016 ve Exchange 2019 desteği içermelidir.
21. Yedekleme yazılımı sağladığı ajan yardımıyla mailbox yedeği almaksızın, Exchange sunucuya ait yedeklenen veritabanı üzerinden e-posta bazında geri dönüşe imkân sağlamalıdır. Yedekleme yazılımı bu operasyonu Exchange üzerinde Recovery Storage Group ya da Recovery Database yaratmadan gerçekleştirebilmelidir.
22. Yedekleme yazılımı sağladığı tek bir ajan yardımıyla Microsoft Active Directory yedeklemesini yapabilmelidir. Aynı ajanı kullanarak Active Directory objelerini sistemi durdurmaya gerek kalmadan çevrimiçi olarak geri dönebilmelidir.
23. Yedekleme yazılımı sağladığı ajan yardımıyla Microsoft SharePoint Server dökümanları için obje tabanlı geri dönüşe imkân vermelidir.
24. Yedekleme yazılımı VMware ESX (6.x, 7.x) ve Microsoft Hyper-V 2012, 2016, 2019, 2022 sanallaştırma teknolojilerini desteklemelidir. Bu teknolojilerle entegre olarak klasik yedekleme metodları kullanmaksızın (sanal makine içine ajan kurmadan) çalışmakta olan sanal makinelerin yedeklerini alabilmelidir.
25. Yedekleme yazılımı VMware/Hyper-V ortamında alacağı tek yedekle hem sanal makine seviyesinde hem de obje seviyesinde (dosya ve dizin) geri dönüş olanağı sağlayan çeşitli betiklere dayalı olmayan entegre bir çözüm sağlamalıdır. Tüm yedekleme ve geri dönme operasyonları sadece grafik arayüz kullanılarak gerçekleştirilebilmelidir.
26. Yedekleme yazılımı sanal makineler yedeğini alırken sanal makine içinde çalışan Active Directory, Exchange, SQL uygulamalarında tutarlı yedeğini alabilmelidir. Alınan bu tek yedekten sanal makinenin hem tamamı hem de sanal makine içinde çalışan bahsi geçen uygulamalar için obje temelli (e-posta, veritabanı vs.) geriye dönüş sağlamalıdır.
27. Yedekleme yazılımı VMware üzerindeki sanal makine yedeklerinin durumunu vCenter arayüzü üzerinden takip edilmesini sağlayacak bir eklenti sağlamalıdır.
28. Yedekleme yazılımı fiziksel sunucuların yedeklerini aldığı sırada eş zamanlı olarak VMware ve Hyper-V sanallaştırma platformlarında çalışacak şekilde dönüşümünü gerçekleştirebilmelidir.
29. Yedekleme yazılımı daha önceden yedeği alınmış bir fiziksel sunucuyu VMware ve Hyper-V sanallaştırma platformlarında çalışacak şekilde dönüşümünü sağlayabilmelidir.
30. Yedekleme yazılımı sunucuları imaj temelli olarak yedekleyebilmelidir. Gerektiği durumda bu imaj kullanılarak farklı donanımlara geri dönme ve sanal platformlara dönüşüm gerçekleştirilebilmelidir.
31. Yedekleme yazılımı doğrudan kullanıma hazır, entegrasyon gerektirmeyen bir tekilleştirme çözümü sunmalıdır.
32. Yedekleme yazılımı tekilleştirme operasyonunu hem istemci (kaynak) üzerinde hem de yedekleme sunucusu üzerinde gerçekleştirebilmelidir.
33. Yedekleme yazılımı kaynakta tekilleştirmeyi, yedeklenecek bilgisayar üzerine ekstra yük oluşturabilecek media sunucu veya storage node benzeri bir yedekleme yazılım sunucu paketi kurmadan, yedekleme yazılımının daha az kaynak tüketen istemci paketini kurarak yapmalıdır.
34. Yedekleme yazılımı tekilleştirme operasyonunu yedeklenmiş tüm sanal makinalar için global şekilde yapmalıdır.
35. Yedekleme yazılımı hem Windows hem de Linux sistemler için kaynakta tekilleştirmeyi desteklemelidir.
36. Yedekleme sunucusu üzerinde gerçekleştirilen tekilleştirme ara bir yedekleme ya da tampon depolama alanı gerektirmeksizin, doğrudan (inline) yapılabilmelidir.
37. Tekilleştirme çözümü herhangi bir disk ünitesinin donanım olarak bütünleşik bir parçası olmamalıdır. Farklı bağlantı tiplerini (FC, iSCSI) desteklemelidir.
38. Tekilleştirme çözümü farklı konumlara (lokasyon/site) IP üzerinden kopyalamayı (replikasyon) desteklemeli ve bu sayede kurumun yedekleme altyapısı için bir felaket kurtarma çözümü oluşturulmasına imkân sağlayabilmelidir.
39. Yedekleme yazılımı yedeklenecek kapasite temelli lisanslama ile temin edilebildiği gibi sanal ortamlar için işlemci sayısına göre de lisanslanabilme tercihi sunabilmelidir.
40. Yedekleme yazılımı üreticisinin Türkiye’de yerel bir ofisi bulunmalıdır.
41. Yedekleme yazılımının KVKK gereksinimlerinin karşılanmasında yardımcı fonksiyonları olmalıdır. TC Kimlik Numaraları sisteme toplu ya da tek tek girilerek yedeklenmiş veride bu bilgilere erişim engellenebilmelidir.
42. Yedekleme yazılımının yedekleri tuttuğu disk alanı ransomware (fidye) saldırılarına karşı yazılımın kendisi tarafından korunmalıdır.
43. Teklif edilecek ürün en az 3 yıl üretici tarafından desteklenmeli ve güncelleştirmeleri alabiliyor olmalıdır.

**ANAHTAR 1 ADET**

1. Anahtar üzerinde en az 48 adet 10Gb/s RJ45, 2 adet 40Gb/s QSFP+ ve 4 adet 100Gb/s QSFP28 hız desteği olan yuva bulunmalıdır ve tüm bu portlar takılı olarak teklif edilmelidir. Tüm portlar kesintisiz (non-blocking) çalışacak şekilde teklif edilmelidir.
2. Uplink portlarına ise en az 40GBase- SR4, 40GBase-LR4, veya 100GBase-SR4, 100GBase-LR4 modül takılabilmelidir.
3. Uplink portları ihtiyaç halinde uygun kablolar kullanılarak 4 x 10Gb/s veya 4 x25Gb/s hızında kullanılabilmelidir. Bu sayede cihaz üzerinde 72 adet bağlantı elde edilebilecektir.
4. Cihazin backplane kapasitesi 1760 Gbps degerinden az olmamalıdır.
5. Cihazin data iletim kapasitesi 1320 milyon pps değerinden az olmamalıdır.
6. Adres tablosunda en az 270.000 adet MAC adresi destegi olmalıdır.
7. Yönlendirme tablosunda en az 200.000 adet IPV4 ve en az 130.000 IPv6 yön bilgisi tutulabilmelidir.
8. Birden fazla konfigürasyon dosyası tutulması için yeterli Flash bellek ile teklif edilmelidir.
9. Cihazın üzerinde en az 4GB RAM olmalıdır.
10. Cihazın üzerindeki paket buffer miktarı 12MB’dan az olmamalıdır.
11. Cihazın işletim sisteminin güncellenmesi esnasında yedeklilik için birbirinden bağımsız iki imaj desteği olmalıdır.
12. VRRP veya benzeri bir ağ gecidi yedekleme mekanizması desteği olmalıdır, bu özellik çalışabilecek halde bir lisans ile teklif edilmelidir.
13. Aynı tipte iki switch’in layer2 seviyesinde aktif aktif olarak çalışması için gerekli olan Multi Chassis Link aggregation vb bir protokol desteği olmalıdır, bu özellik çalışabilecek halde bir lisans ile teklif edilmelidir.
14. IEEE 802.1Q (4,000 VLAN ID) VLAN ID’si işaretleme desteği ve en az 4000 adet port bazında VLAN tanımlanabilmelidir.
15. IEEE 802.1D Spanning Tree protokolü desteği olmalıdır.
16. Remote Span desteği olmalıdır.
17. VRF-lite desteği olmalıdır.
18. VXLAN desteği olmalıdır.
19. IEEE 802.1w Rapid Convergence/ Reconfiguration Spanning Tree protokolü desteği olmalıdır.
20. 9K byte büyüklüğüne kadar iletim birimi (Jumbo Frame) desteği bulunmalıdır.
21. Layer 3 yönlendirme desteklenecektir. Teklif edilecek cihaz, ilgili ailenin en üst lisanslama modeli ile teklif edilecektir. Dinamik routing protokolleri de, OSPF ve BGP dahil desteklenecek sekilde lisanslı ve kullanılabilir olacaktır. Ayrıca teklif edilecek cihaz bu protokollerin çalışması için harici bir cihaza gerek duymamalıdır. Tek başına kullanıldığında da bu özellikleri sağlayabilmelidir.
22. Yeni jenerasyon IPv6 desteği bulunmalıdır. IPv4 protokolünden IPv6 protokolüne geçiş için her iki protokolün kullanımına imkan vermelidir.
23. RADIUS ve TACACS+ protokolleri ile kimlik tanımlama özelliklerini desteklemelidir.
24. sFlow veya NetFlow gibi veri akışı izleme protokollerinin en az birinin desteği bulunmalıdır.
25. Teklif edilecek cihaz Data Center sınıfı cihaz olmalı, sipariş esnasında tercihe göre hava akış yönü değiştirilebilir olmalıdır.
26. Teklif edilecek cihaz 7x24 saat esasında arıza kaydı açılabilecek seviyede ek bir üretici destek paketi ile birlikte teklif edilmelidir. Bu destek paketinin süresi 3 yıldan az olmamalıdır. Bu destek iş ortağı tarafından verilen destek değil, üreticinin sağladığı uluslararası bir destek olmalıdır.
27. Cihazın üzerinde yedek güç kaynağı desteği olmalı ve takılı olarak teklif edilmelidir.

**42U 80X100 DİKİLİ TİP RACK KABİN -1 ADET**

* 1. 19” Rack kabinet ve aksesuarlarının üretiminde ISO 9001:2008 kalite güvence sistemi kullanılmalıdır..
  2. 19” Rack kabin sistemleri, EN 15371 standartlarını içeren TSE veya dengi bir kuruluş tarafından verilmiş belgeye sahip olmalıdır.
  3. Kabinet 42U Genişlik : 800mm Derinlik : 1000mm olarak imal edilmelidir.
  4. Ana şase ve profil yapıları; esneksel (x, y, z) mukavemeti EN 15371 /5.2.1 ve 5.2.2, dış darbelere dayanıklılığı EN 15371 / 5.3.3 sağlayacak şekilde imal ve test edilmiş olmalıdır. Dinamik yük, titreşim ve mekanik darbe test sonuçları TSE veya dengi bir kuruluş tarafından belgelenmiş olmalıdır.
  5. Kabinetlerin ana profil yapısı “U” profil mantığında imal edilmeli ve kaynaklı yapıda olmalıdır.
  6. Ön ve arka panel; kabin sağlamlığını ve mukavemetini arttıracak; monoblok şeklinde, kaynaklı yapıya sahip olmalıdır. Profiller; ön ve arka panele bağlantılı vidalı ve/veya kaynaklı olarak imal edilmelidir.
  7. Kabinetlerde hava sikülasyonunu sağlamak için 4 fanlı dijital termostatlı on/off anahtarlı tavana monte edilmiş havalandırma sistemi bulunacaktır.
  8. Kabinetlerde kablo girişleri Üstten ve altından sağlanabilir şekilde imalat yapılmalıdır.
  9. Kabinetler’de önler frenli arkalar ise döner tip tekerleklere sahip olmalıdır.
  10. Kabinetin içerisinde en az 1 adet olmak üzere Alümunyim profil gövdeli 1x16A sigorta korumalı 6’lı sigortalı priz modülü bulunmalıdır.
  11. Her bir kabinette kabloların için Dikey kapaklı organizer modülü Sağ/sol 1:Set Organizer bulunmalıdır.
  12. Kabinetlerin yan kapakları kilitnebilir yapıda olmalıdır. Tüm kabinetler aynı şifreli anahtar ile açılabilmedir.
  13. Arka kapak; 130 derece açılabilir, sökülebilir, kilitlenebilir, yapıya sahip olmalıdır.
  14. Yan kapaklar; tek parça tırnaklı geçme yapıda aynı zamanda kilitlenebilir yapıda ve yan yana bağlanabilir özellikte imal edilmiş olmalıdır.
  15. Ön kapak dört tarafı Alüminyum çerçeve içerisinde pleksglas cam olmalıdır.
  16. 19 inç montaj dikmeleri; önde 2 adet, arkada 2 adet olacak şekilde ve kabinet derinliği boyunca ileri ve geri hareket edebilecek U ölçüleri markalanmış dikme üzerinde belirtilecek ve yük taşıma minimum olarak 400kg taşıyabilecek şekilde 1,5mm Galvaniz sactan imal edilmiş şekilde imal ve montaj edilmiş olmalıdır.
  17. Kabinet elektrostatik RAL 9005 Texture Siyah veya RAL 7035 Wrinkle Beyaz toz boya ile boyanmalıdır.
  18. Her bir kabinetteM6 patch panel vida somun ( 1 Pk:50 adet) verilecektir.
  19. Kabinet boyası darbelere karşı yüksek mukavemeti sağlayacak şekilde idarenin onay verdiği renkte boyanmalıdır.Minimum 700 saatlik tuz testine dayanımlı olmalıdır ve test sonuç raporları belgelenmelidir.

**TAPE BACKUP ÜNİTESİ 1 ADET**

1. “Tape Library” özelliğinde olacaktır.

2. 19 (on dokuz) inç genişliğinde ve kabinet tipinde olacaktır. Kabinet bağlantı kızakları ve aparatları ile beraber teslim edilecektir.

3. Kafa (drive) sayısı en az 1 (bir) olacaktır.

4. En az LTO-8 sürücü teknolojisine sahip olacaktır.

5. Bağlantı arayüzleri FC olacaktır.

6. En az 32 (otuz iki) adet kartuş yuvası bulunacaktır.

7. En fazla 3 (üç) U yüksekliğinde olacaktır.

8. En az 2 (iki) adet güç ünitesi olacaktır.

9. Web arayüzünden yönetilebilir olacaktır.

10. Her bir teyp ünitesi ile birlikte teklif edilecek teyp ünitesi ile aynı marka orijinal en az 40 (kırk) adet en az LTO-8 kartuş, en az 200 (iki yüz) adet barkod etiketi ve teklif edilecek teyp ünitesi ile aynı marka orijinal en az 1 (bir) adet temizleme kartuşu verilecektir.

11. Ön tarafında LCD/LED panel bulunacaktır.

12. Tümleşik veya kart şeklinde en az bir adet en az 10/100 (on/yüz) Mbps hızları ile uyumlu RJ-45 tipinde Ethernet çıkışı bulunacaktır.

13. Cihaz en az 3 yıl boyunca ertesi iş günü üretici garantisine sahip olacaktır.

# GÜVENLİK DUVARI SİSTEMİ 1 ADET

Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.

* 1. Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;
     1. Güvenlik Duvarı (Firewall)
     2. IPSec VPN Sonlandırma Sistemi
     3. SSL VPN Sonlandırma Sistemi
     4. Saldırı Tespit ve Engelleme Sistemi (IPS)
     5. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
     6. Virüs/Zararlı İçerik Kontrolü
     7. URL Kategori Filtreleme
     8. Bant genişliği yönetimi

Özelliklerine sahip olmalıdır.

* 1. 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.
  2. 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.
  3. Yedeklilik konfügrasyonunda her segment için güvenlik duvarı üzerinde set edilecek Ip sayısı 1 (bir) adet olabilmelidir. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.
  4. Sistem üzerinde en az 4 adet SFP, 16 Adet RJ45 1Gbit/s interface olmalıdır.
  5. Sistem üzerinde en az 2 adet SFP+ 10Gbit/s interface olmalıdır.
  6. Sistem üzerinde 2 adet yedekli AC güç kaynağı bulunmalıdır.
  7. Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.
  8. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır, anti-spoof özelliğine sahip olmalıdır.
  9. 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.
  10. 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.
  11. 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.
  12. Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
      1. SPI (stateful packet inspection),
      2. Saldırı Tespit ve Engelleme Sistemi (IPS)
      3. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
      4. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
      5. URL Kategori Filtreleme
  13. Routing modda aşağıdaki özellikleri sağlamalıdır;
      1. SPI (stateful packet inspection),
      2. IPSec VPN Sonlandırma,
      3. SSL VPN Sonlandırma,
      4. Saldırı Tespit ve Engelleme Sistemi (IPS)
      5. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
      6. Virüs/Zararlı İçerik Kontrolü
      7. URL Kategori Filtreleme
      8. Bant genişliği kontrolü
      9. Statik yönlendirme (static routing),
      10. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
      11. Sunucu yük dengeleme
  14. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.
  15. Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.
  16. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.
  17. Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü (interface) ve/veya zone bazlı yazılabilmelidir.
  18. Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.
  19. Kullanıcı bazında NAT kuralı yazılabilmelidir.
  20. Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.
      1. Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
      2. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
      3. 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.
      4. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
      5. Uygulama bazında bant genişliği kontrolü yapabilmelidir.
      6. 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.
  21. Ağ Güvenlik Duvarı Sistemi kendi üzerinde tanımlanan kullanıcı veritabanı, harici RADIUS ve LDAP sunucuları üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir. SSLVPN, client-site IPSEC VPN, internet erişimi gibi senaryolar için bu özellik kural bazlı devreye alınabilmeli ve kullanıcı takibi (kullanıcı ismi, grubu, yarattığı trafik, kalan süre vb..) gibi detaylar GUI üzerinden gözlemlenebilmelidir.
  22. Aktif dizin entegrasyonu ağ güvenlik duvarı üzerinden sorgu çekme yöntemiyle veya domain üyesi herhangi bir sunucu üzerine kurulacak ajan yardımıyla gerçekleşebilmelidir. Sistemin temel çalışmasında son kullanıcı makinalarına bir yazılım kurulması ihtiyacı bulunmamalıdır.
  23. Domain entegrasyonu sonucunda bir nedenden (Windows ortamı vb..) firewall ile senkronize edilememiş kullanıcıların firewall üzerinden geçerken anında tanınabilmesi için NTLMv2 gibi güvenli alternatif yöntemler kullanılabilmelidir.
  24. Ağ Güvenlik Duvarı Sistemi aktif dizin ile entegre edildiğinde ip/subnet/vlan/zone bazlı tanımlamalara ek olarak kullanıcı ve grup bazlı güvenlik politikaları yazılmasını desteklemelidir. Kullanıcı ve grup tanımlamaları politika ekranından arkadaki aktif dizin üzerinden otomatik filtrelenerek getirilen user, security group veya OU tanımları içerisinden çoklu-seçim ile tek adımda gerçekleştirilebilmelidir. Bu sayede farklı kullanıcı profillerine farklı güvenlik politikaları uygulanabilmelidir.
  25. Ağ Güvenlik Duvarı Sistemi üzerinde güvenlik politikaları ip/subnet, interface (fiziksel/VLAN), zone, kullanıcı, grup (OU veya Security Group) haricinde cihaz tipi bazlı da yazılabilmelidir. Windows, Linux, Android, Iphone vb.. gibi hazır tanımlı cihaz kategoriler haricinde kişiselliştirilmiş cihaz tanımlamaları (el terminalleri, printer vb..) yapılabilmelidir.

* 1. 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.
  2. Ağ Güvenlik Duvarı Sistemi Web 2.0 uygulamaları içerisindeki alt uygulamaları (facebook.chat, facebook.games vb.. gibi) ayırt edebilmeli ve sosyal medya uygulamalarına read-only erişimi (facebook açılsın ama oyun oynanamasın, chat fonksiyonu kullanılamasin vb.. gibi) mümkün kılabilmelidir.
  3. Ağ Güvenlik Duvarı Sistemi uygulama veya kategori bazlı blok, reset, allow, log, karantina aksiyonlarını alabilmelidir.
  4. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.
  5. Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.
  6. 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.
  7. IPS sistemi en az 7000 (yedibin) imzaya sahip olmalıdır.
  8. 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.
  9. Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını ve aynı zamanda atak yapılan sistemlere olan erişimi belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapılan sistem olası ataklara karşı koruma altına alınabilmelidir
  10. Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkân sağlamalıdır.
  11. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.
  12. Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.
  13. 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.
  14. SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.
  15. SSL VPN özelliği en az 500 kullanıcı lisansı ile teklif edilecektir.
  16. 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.
  17. 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.
  18. 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
  19. Kaynak (IP ve/veya kullanıcı), hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.
  20. 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.
  21. Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı domain adı filtreleme politikaları set edilebilmelidir.
  22. Sistem üzerinde en az 70 adet URL kategorisi bulunmalıdır, en az 250milyon URL sınıflandırılmış olmalıdır.
  23. Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.
  24. 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.
  25. Https üzerinden erişilmeye çalışılan domain adreslerinin (örneğin www.abc.com) engellemesi sertifika kullanımı olmadan gerçekleştirilebilmelidir.
  26. SSL trafiğini kendi üzerinde yaratılan bir sertifikayı yada farklı bir CA den alınmış yeterli özelliklere sahip bir sertifika ile inceleyebilmelidir. Bu sayede sadece domain bazında değil, URL bazında (Örneğin: [www.abc.com/deneme](http://www.abc.com/deneme)/test.php) engelleme yapabilmelidir. URL kategorileri bazında SSL incelemeye girmeyecek domainler belirlenebilmelidir.
  27. URL/Application kontrol/Anivirus filtreleme uyarı ekranları özelleştirilebilecektir.
  28. 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.
  29. Sistem IPv6 için DDoS profiline sahip olmalıdır.
  30. Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
      1. Seri bağlantı ile konsol port üzerinden,
      2. Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
      3. SSH bağlantı ile komut satırı (commandline) üzerinden
  31. Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir
  32. Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.
  33. Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.
  34. Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.
  35. Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.
  36. Sistem, içeri doğru NAT Load-Balance özelliği ile internetten gelen istekleri birden fazla sunucuya yönlendirebilmelidir. Örneğin, iç ağda bulunan ve aynı servisi veren iki web server veya terminal server arasında trafik paylaşımı bu özellik sayesinde yapılabilmelidir. Eğer web server veya terminal server‘lardan birisi devre dışı kalırsa diğer web server veya terminal server herhangi bir müdahaleye gerek kalmadan hizmetine devam edebilmelidir.
      1. Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP, Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.
      2. Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.
      3. HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.
      4. SSL bağlantıları için SSL Offloading özelliği olmalıdır.
      5. Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:
         1. Kaynak Ip hash bilgisi
         2. Round robin
         3. Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak
         4. Aktif durumda olan gerçek sunuculardan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi
         5. Ping paketlerine verilen cevaplar esas alınması
         6. Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak
      6. Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin <http://10.31.101.30/test_page.htm> adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.
  37. Explicit proxy özelliği desteklenmelidir.
  38. Sistem TCP eşik değeri temelli DoS/DDoS koruması saglayabilmelidir.
  39. 10 adet sanal güvenlik duvarı desteği standart lisans ile verilebilmelidir.
  40. Sistem WAN tarafında optimizasyon ve yük dağılımı desteği olmalıdır.
  41. Sistem wan link load balance özelliğine sahip olmalıdır ve internet çıkışı oransal olarak ilgili dış hatlara yönlendirilebilmelidir.
  42. Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.
  43. Web cache özelliği olmalıdır.
  44. Sistem WAF (Web Application Firewall) profillerini desteklemelidir. Bu oluşturulan profiller kural temelli olarak tanımlanabilmelidir.
  45. Web cache communication Protocol (WCCP/ICAP) desteği olmalıdır.
  46. Sistem WAF (Web Application Firewall) profillerini desteklemelidir. Bu oluşturulan profiller kural temelli olarak tanımlanabilmelidir.
  47. Sistem VOIP güvenlik profillerine sahip olmalıdır ve kural temelli olarak uygulanabilmelidir.

# Güvenlik Duvarı Performans Değerleri

* 1. Teklif edilen Ağ Güvenlik Duvarı, yedekli aktif-aktif/aktif-pasif olarak çalışabilme özelliğine sahip olmalıdır.
  2. Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, 1518/512/64 Byte IP paket büyüklüklerinin hepsi için en az 10 Gbit/sec performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
  3. Sistem aynı anda en az 1 milyon oturumu desteklemeli ve saniyede en az 50 bin yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün dokümanlarında belirtilmiş olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
  4. Güvenlik Duvarı Sistemi en az 10 Gbit 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. Güvenlik Duvarı Sistemi en az 1Gbit SSL inspection throughput değerine sahip olmalıdır. Bu performans degieri IPS açık iken HTTP trafiğinin TLS v1.2 with AES256-SHA şifrelemesi ile elde edilmelidir. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
  6. Sistem Site-to-Site için en az 1000 adet, Client to site için 2000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir
  7. Sistem 2Gbit/sec Enterprise MIX 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.
  8. Sistem 1Gbit/sec Thread Prevention (Malware kontrol, Application kontrol, IPS) throughput performans değerine Enterprise trafic MIX veya gerçek trafik değeri olarak sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
  9. Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

**GÜÇ KAYNAĞI UPS 2 ADET**

1. KGK, elektronik ekipmanları korumak için dizayn edilmiş çift çevrimli online topoloji ile

aşırı gerilim ve frekans regülasyonuna sahip olmalıdır.

2. KGK, dahili bypass ve giriş güç faktörü düzeltme özelliğine sahip olmalıdır.

3. KGK’nın birincil bölümleri; giriş bağlantı kesme ve filtre bölümü, giriş güç faktörü

düzelme bölümü, enerji depolama bölümü (DC bus kapasitör bankası), çıkış güç çevirici

bölümü, bypass ve akü şarj edici. Güç modülünün kontrolü ve hata tespit mantığı

mikrodenetleyici tabanlı olmalıdır.

a. Giriş bağlantı kesme ve filtre aşaması, bir giriş geri besleme rölesi, giriş filtresi,

geçici baskılama ve akü seçme anahtarları içermelidir.

b. Giriş güç faktörü düzeltici güç aşaması izole edilmemiş güç faktörü düzeltici ve

AC/DC dönüştürücüler içermelidir. Bu dönüştürücüler çok geniş bir giriş voltaj aralığında

veya nominal DC batarya voltajında tam güçle çalışabilmelidir.

c. Enerji saklama aşaması; bataryadan çevrim içi ve tersine kesintisiz geçişler ile

düşük ve yüksek frekanslı güç aşamaları dalgalanmalarını gidermek için ayrılmış

bir DC bus kapasitörü içermelidir.

d. Çıkış gücü (invertör) kademesi direkt olarak DC bus üzerinden çalışarak 200,

230 veya 240 Vac çıkış yapılandırılabilir bir AC çıkış voltajı üretebilmelidir. Ünite min. 10KVA olmalıdır.

e. KGK, DC veriyolundan çalışan bir akü şarj edici içermelidir.

f. KGK aküleri modüler olmalı çalışırken değiştirilebilir ve kullanıcı tarafından değiştirilebilir olmalıdır. KGK, uzun süreli bir elektrik kesintisi sonrasında akünün şarj edilmesini beklemeden derhal yeniden başlatılabilmelidir.

4. KGK, herhangi bir korumadan ödün vermeden, ENERGY STAR® niteliklerini aşan çok

yüksek çalışma verimliliği (genelde %98) sağlayabilmelidir.

**KURULUM**

1. Şartnamede teklif edilen bütün ürünler birbirleriyle entegre edilerek sistem çalışır halde kurulumu yapılacaktır.
2. Şartnamede teklif edilecek bütün ürünler için gereken lisanslar teklif veren tarafından karşılanacaktır. Üç yıllık süre için lisansların kullanım hakları teslim edilecektir.
3. Şartnamede teklif edilecek olan ürünler yeni nesil ürünler olacak ve üretici firmaların desteklerinin en az beş yıl daha devam ediyor olması şartı aranacaktır.