KTO KARATAY ÜNİVERSİTESİ
SA-24-04 NOLU BİLGİSAYAR VE YAZILIM LİSANSI ALIMI İHALESİ
ÜRÜN TEKNİK ŞARTNAMESİ

1. KONU

Bu şartname KTO Karatay Üniversitesi Bilgi İşlem Direktörlüğü Bilgi Teknolojileri alanında ihtiyaçlarına binaen bu şartnamede belirtilen donanım, yazılım ve lisans satın alınması ve sorunsuz çalışır şekilde teslim edilmesini içermektedir.

TEKLİF EDİLECEK ÜRÜNLER

1- Masaüstü Bilgisayar (60 Adet)
2- iMac (40 Adet)
3- Firewall (1 Adet)
4- Waf (1 Adet)
5- Analyzer (1 Adet)
6- Hiper Bütünleşik Sistem (3 Node)
7- Projeksiyon (3 Adet)
8- Antivirüs (1000 Kullanıcı)

1 MASAÜSTÜ İŞ İSTASYONU BİLGİSAYAR (60 ADET)

1. Teklif edilen bilgisayar markasının **kurumsal** ürün ailesinden olacaktır. Bu markanın internet sitesinden görülebilecektir.
2. Teklif edilen ürün 5 Yıl Marka garantili yerinde destek verilecektir. (5 Year Next Business Day Onsite Desktop Hardware Support)
3. Bilgisayarın işlemcisi en az 13. nesil Intel Core i7-13700 serisi olmalıdır.
4. Teklif edilen üründe NVIDIA grafik kartı, en az 8GB GDDR6X belleği ile birlikte, grafik yoğun uygulamalar ve profesyonel işler için yeterli performansı sunmalıdır.
5. Anakart üzerinde bütünleşik Autosense 10/100/1000 Mbps hızlarında RJ45 konektör girişli Wake-On-LAN destekli ethernet kartı bulunacaktır.
6. Anakart üzerinde en az 2 adet ram bellek yuvası bulunmalıdır.
7. Anakart üzerinde en az 1 adet DVI/DP veya en az 1 adet HDMI port bulunmalıdır.
8. Aynı anda en az 2 monitöre birden görüntü verebilmelidir.
9. Bilgisayarın en az **2 x 16GB DDR5** 4400 MHz ECC 32 Gb ram belleği bulunmalıdır.
10. Bellekler **DDR5 4400Mhz** hızını desteklemelidir.
11. Maksimum bellek kapasitesi 128GB olmalıdır.
12. En az 512GB PCIe NVMe SSD + 2TB 3.5” SATA HDD depolama birimleri, hızlı veri erişimi ve geniş depolama kapasitesine sahip olmalıdır.
13. Bilgisayarda ses portu bulunmalıdır.
14. Bilgisayarda en az 4 adet USB girişi olmalı ve bunlardan en az 2 tanesi USB 3.2 desteklemelidir.
15. Bilgisayardaki USB portlarından bir tanesi Type-C formatında olmalıdır.
16. Her bir bilgisayar ile beraber ürün ile aynı marka USB Türkçe Q klavye verilmedir.
17. Her bir bilgisayar ile beraber ürün ile aynı marka USB sahip optik mouse verilmedir.
18. Bilgisayar ile aynı marka 1920x1080 çözünürlülük desteği olan LED veya IPS teknolojisine sahip DVI veya DP, D-Sub, çıkışları olan siyah renk 24” Monitör ürün ile beraber teklif edilmelidir. Teklif edilen ürün, monitör ve kasa arasında kullanılan veya kullanılacak olan ara bağlantı kablosunu da içermelidir.
19. Cihaz ilk teslim aşamasından sonra 3 iş günü içinde arızalı olduğu tespit edilirse 2 iş günü içerisinde yenisiyle değiştirilmedir.
20. Teklif edilen üründe en az 400 W power bulunmalıdır.
21. Teslimat sırasında kutu hasarlı veya açılmış koliler kabul edilmeyecektir.
22. İşletim sistemi freedos olacaktır.
23. Bu teknik şartnamedeki maddelerde belirtilen özellikler asgari olup, şartnamedeki özellikleri sağlamak şartıyla daha üst özellikleri kapsayan ürünler teklif edilebilir.
24. **Teklifle birlikte epeat silver (epeatın resmi sayfasından görüntü alınarak eklenecektir) ve energ star belgeleri olacaktır.**

2- iMAC BİLGİSAYAR (40 adet)

1. Teklif edilen bilgisayar markasının **kurumsal** ürün ailesinden olacaktır. Bu durumun markanın internet sitesinden görülebilecektir.
2. Bilgisayar en az **2 yıl** garantili olmalıdır, bu garanti distribütör ya da üretici tarafından da taahhüt edilmelidir. Garanti belgesi teklifle birlikte sunulmalıdır.
3. Bilgisayarın işlemcisi en az 8 CPU 8 GPU olmalıdır.
4. En az **512 GB SSD** kapasiteye sahip disk olmalıdır.
5. Bilgisayarın en **az 16GB** ram belleği bulunmalıdır.
6. Cihaz Minimum **24”** ekran boyutunda olmalıdır.
7. Bilgisayarda ses portu bulunmalıdır.
8. Renk beyaz olmalıdır.
9. Bilgisayarlarda dahili hoparlör, dahili mikrofon ve dahili kamera bulunmalıdır.
10. Her bir bilgisayar ile beraber ürün ile aynı marka USB Türkçe Q klavye verilmedir.
11. Her bir bilgisayar ile beraber ürün ile aynı marka USB sahip optik mouse verilmedir.
12. Cihaz ilk teslim aşamasından sonra 3 iş günü içinde arızalı olduğu tespit edilirse 2 iş günü içerisinde yenisiyle değiştirilmedir.
13. Teslimat sırasına kutu hasarlı veya açılmış koliler kabul edilmeyecektir
14. Teklifle birlikte epeat silver (epeatın resmi sayfasından görüntü alınarak eklenecektir) ve energ star belgeleri olacaktır.

3- FİREWALL CİHAZI VE LİSANSI (1 ADET)

Ağ Güvenlik Duvarı Sistemi

Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.

1.1. Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;
1.1.1. Güvenlik Duvarı (Firewall)
1.1.2. IPSec VPN Sonlandırma Sistemi
1.1.3. SSL VPN Sonlandırma Sistemi
1.1.4. Saldırı Tespit ve Engelleme Sistemi (IPS)
1.1.5. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
1.1.6. Virüs/Zararlı İçerik Kontrolü
1.1.7. URL Kategori Filtreleme
1.1.8. Bant genişliği yönetimi

Özelliklerine sahip olmalıdır.

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.

Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, her hâlükârda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.

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.

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.

Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.

Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır

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.

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.

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.

Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
1.1.9. SPI (stateful packet inspection),
1.1.10. Saldırı Tespit ve Engelleme Sistemi (IPS)
1.1.11. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
1.1.12. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
1.1.13. URL Kategori Filtreleme

Routing modda aşağıdaki özellikleri sağlamalıdır;
1.1.14. SPI (stateful packet inspection),
1.1.15. IPSec VPN Sonlandırma,
1.1.16. SSL VPN Sonlandırma,
1.1.17. Saldırı Tespit ve Engelleme Sistemi (IPS)
1.1.18. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
1.1.19. Virüs/Zararlı İçerik Kontrolü
1.1.20. URL Kategori Filtreleme
1.1.21. Bant genişliği kontrolü
1.1.22. Statik yönlendirme (static routing),
1.1.23. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
1.1.24. Sunucu yük dengeleme
1.1.25. WIFI Access Point kontrolcüsü
1.1.26. WAN optimizasyon
1.1.27. Web Cache

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

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

Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.

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

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

Kullanıcı bazında NAT kuralı yazılabilmelidir.

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

1.1.28. Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
1.1.29. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
1.1.30. 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.

1.1.31. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
1.1.32. Uygulama bazında bant genişliği kontrolü yapabilmelidir.
1.1.33. 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.

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

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.

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

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

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.

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.

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

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

Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.

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.

SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.

SSL VPN özelliği **en az 10.000 kullanıcı lisansı** ile teklif edilecektir.

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.

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.

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

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

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.

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

Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.

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

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 3 YIL geçerli olacak şekilde teklif edilmelidir.

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.

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

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

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.

URL filtreleme uyarı ekranları özelleştirilebilecektir.

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.

Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
1.1.34. Seri bağlantı ile konsol port üzerinden,
1.1.35. Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
1.1.36. SSH bağlantı ile komut satırı (commandline) üzerinden

Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir

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

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

Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel “Network Firewalls” için “Gartner Magic Quadrant” tablosunda yer almalıdır.

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

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

1.1.37. Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP, Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.
1.1.38. Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.
1.1.39. HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.
1.1.40. SSL bağlantıları için SSL Offloading özelliği olmalıdır.
1.1.41. Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:
1.1.41.1. Kaynak Ip hash bilgisi
1.1.41.2. Round robin
1.1.41.3. Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak
1.1.41.4. Aktif durumda olan gerçek sunuculardan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi
1.1.41.5. Ping paketlerine verilen cevaplar esas alınması
1.1.41.6. Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak

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

Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.

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

Wan optimizasyon özelliklerine sahip olacaktır.
Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.

a. Güvenlik Duvarı Performans Değerleri

Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda en az 130 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.

Her bir Ağ Güvenlik Duvarı ünitesi Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az **10,5 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 **11,5 Gbps** olmalıdır.

Sistem aynı anda en az 8 milyon oturumu desteklemeli ve saniyede en az 550.000 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.

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.

Sistem Site-to-Site için en az 2.000 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.

1.2. Sistem 14 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.

Sistem üzerinde;

1.2.1. En az 4 adet 25GE SFP28/10GE SFP+ ara yüz bulunmalıdır.
1.2.2. En az 4 adet 10GE SFP+ ara yüz bulunmalıdır.
1.2.3. En az 8 adet 1GE SFP ara yüz bulunmalıdır.
1.2.4. En az 16 adet 1GE RJ45 ara yüz bulunmalıdır.

Sistem Syslog Sunuculara ve Kayıt/Raporlama Sistemine kayıt gönderebilmelidir.

Sistemin; Firewall ve 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 Ana cihaz sistemle birlikte verilmelidir.

1.2.5. Teklif edilen ürünün kurulumu ve devreye alım işi üniversite tarafından belirlenecek kişi yada kişiler ile birlikte yapılıp sorunsuz bir şekilde teslim edilecektir.

4- WAF (1 Adet)

1. PERFORMANS

1.1. WAF ürünü Compression fonksiyonunu ve SSL/TLS trafiğini özel donanım mimarisi üzerinde işlemesi tercih sebebi olacaktır.
1.2. Gelişmiş WAF throughput değerleri üreticinin herkese açık datasheet değerleri içerisinde açıkça belirtilmiş olmalıdır.
1.3. WAF ürünü minimum 500 Mbps HTTP trafiğini, hem request hem de response trafiğini izlerken ve tüm gelişmiş WAF fonksiyonları açık şekilde işleyebilme kapasitesine sahip olmalıdır.
1.4. WAF ürünü en az 4 adet 1GE SFP arayüze sahip olmalıdır.
1.5. WAF ürünü en az 4 adet 1GE RJ45 arayüze sahip olmalıdır.
1.6. WAF ürünü donanım içerisinde en az 64 adet, sertifika, log, politika ve raporlamanın desteklenebileceği birbirinden bağımsız yönetilen sanal ortam özelliğine sahip olmalıdır. Bu sanal ortamlar hem loadbalancing hem de waf özelliklerini birlikte sanallaştırmalı, kısıtlı yönetici profilleri ile bus anal alanlara kontrollü erişim sağlanabilmelidir.
1.7. Sistemin; 24x7 Care, Antivirus, Web Security Service ve IP Reputation fonksiyonlarının 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

2. KONUMLANDIRMA

2.1. WAF ürünü L3 olarak konumlandırılabilmeli, SSL Offload yapabilmeli ve yükü uygulama sunucularına dağıtabilmelidir.
2.2. WAF ürünü L2 (bridge) modda konumlandırılabilmeli, ağda DNS yada IP değişikliğine gerek kalmadan devreye alınabilmeli ve SSL trafiğini de açıp koruma sağlayabilmelidir.
2.3. WAF ürünü offline olarak konumlandırılabilmeli, mirror trafik üzerinden izleme yaparak web trafiğini analiz edebilmeli ve raporlayabilmelidir.
2.4. WAF ürünü offline olarak konumlandırıldığında SSL trafiğini de açabilmelidir.
2.5. WAF ürünü offline olarak konumlandırıldığında dahi saldırı tespit ederse saldırgana RST paketi göndermek suretiyle saldırıyı engelleyebilme özelliğine sahip olmalıdır.
2.6. WAF ürünü bir loadbalancer önüne konumlandırıldığında istek paketlerine XFF header'ı ekleyerek orjinal istemci IP'sini arkaya iletebilmelidir.
2.7. WAF ürünü loadbalancer yada reverse proxy görevi gören bir cihaz ile uygulama sunucuları arasına konumlandırıldığı durumda eğer orjinal client IP (X-Forwarded-For) HTTP header'ları ile birlikte gönderiliyorsa bu IP'yi yorumlayabilmeli, bu IP üzerinden üreticinin istihbarat ağına IP Reputasyon sorgusu yapabilmeli ve Saldırı Loglarında "Source IP" olarak orjinal client IP görüntülenebilmelidir.
2.8. WAF ürünü L2 olarak konumlandırıldığında dahi ağ'da loop oluşmasını engeleyecek senaryolarda kendi MAC adresini yayınlayabilmelidir.
2.9. WAF ürününün MSSP modeli olarak vmware platformu üzerinde PaYG modelini üzerinden geçen trafik yada kullanılan vCPU bazında desteklemesi ve buna göre ücretlendirebiliyor olması tercih sebebidir.

3. YÖNETİM

3.1. WAF ürünü IPv6 desteklemelidir.
3.2. WAF ürünü kendi içerisinde sanallaştırmaya uygun olmalı böylelikle birden fazla uygulama sahibine ayrı ayrı hizmet edebilmeli, farklı uygulamalara farklı yönetici hesapları ile erişime olanak tanıyabilmeli ve raporlayabilmelidir. İlgili kullanıcılar read-only ya da read-write farklı erişim politikalarına tabi tutulabilmelidir.(multitenancy)
3.3. WAF ürününün üçüncü parti web tarama araçları (Acunetix, Qualys vb..) ile entegre olabilmesi tercih sebebi olacaktır, bu araçların çıktılarını içe aktarmaya olanak tanıyarak uygulama özelinde otomatik politika oluşturabilmelidir(virtual patching).
3.4. WAF ürünü coğrafi trafik analizi yapabilmeli ve bunu görsel olarak sunabilmelidir.
3.5. WAF ürünü L2 konumlandırılmış dahi olsa coğrafi trafik analizi yapabilmeli ve coğrafi lokasyon veritabanını internetten güncelleyebilmelidir.
3.6. WAF ürünü trafik ya da atak verisine göre dünya haritası üzerinden sağ klik ile herhangi bir ülkeyi bloklama özelliğine sahip olmalıdır.
3.7. WAF ürünü Aktif-Pasif ve Aktif-Aktif yedekli mimaride çalışmayı desteklemelidir.
3.8. WAF ürünü SSH/HTTPS,TELNET protokollerini kullanarak uzaktan yönetime izin vermelidir.
3.9. WAF ürünü Komut Satırı ve Web Arayüzü yönetim konsolları sunmalıdır.
3.10. WAF ürünü üreticinin kendi fiziksel sunucusunda çalışmalıdır.
3.11. Teklif edilecek WAF ürününün sanal platform desteğinin olması tercih sebebidir.
3.12. WAF ürünü yedekli Güç ünitesi konumlandırılmasına izin vermelidir.
3.13. WAF ürünü koruduğu uygulamalar için topoloji çizebilmelidir. Hangi VIP arkasında hangi sunucular olduğunu belirtebilmelidir.
3.14. WAF ürünü yönetici hesapları için parola politikası özelliğine sahip olmalıdır. Belli uzunluk, büyük harf/küçük harf/rakam/özel karakter, expire time veya aynı anda bağlanabilecek maksimum admin hesabı tanımlanabilmelidir.

4. GÜVENLİK

4.1. WAF ürünü uygulamada kullanılan parametreler için öntanım yapmaya olanak tanıyabilmelidir. Pozitif güvenlik modelini desteklemelidir.
4.2. Güvenlik uzmanı koruma ve öğrenme politikalarını ayrı ayrı düzenleyebilmeli, ikisinden biri üzerinde çalışırken diğerini etkilememelidir.
4.3. WAF ürünü IP reputasyonuna göre otomatik olarak bilinen botnet, malicious hosts, anonymous proxy'ler ve D/DoS kaynaklarını engelleyebilmeli, kısa periyodlarla saldırı yapan IP adreslerini kontrol ederek güncel tehdit olup olmadığını kontrol etmeli ve duruma göre otomatik olarak karalisteye ekleyip çıkarabilmelidir. IP Reputasyonu altında farklı kaynak kategorileri için farklı aksiyon alabilmelidir.
4.4. WAF ürünü yapay zeka tabanlı BOT koruması yapabilmeli, uygulama özelinde hiçbir static tanıma gerek kalmadan tamamen istatistiksel algoritmalar ile BOT davranışlarını tespit edip engelleyebilmelidir.
4.5. WAF ürünü aldatma(deception) tabanlı BOT koruması yapabilmelidir. WAF ürünü koruduğu uygulamada olmayan bir url'i aldatma amaçlı sayfanın içerisine koyacak, bu url'e erişmek isteyen istemcileri BOT olarak taspit edecektir.
4.6. WAF ürünü BOT koruması kapsamında istemcinin klavye ve mouse davranışları üzerinden control sağlayabilmelidir.
4.7. WAF ürünü TOR exit node'larından yapılan erişimleri engelleyebilmelidir. Güncel TOR IP'lerini otomatik olarak kendi istihbarat ağından update edebilmelidir.
4.8. WAF ürünü içerik çalma (Content Scrapping) saldırılarına karşı koruma sağlamalıdır.

4.9. WAF ürünü kendi içerisinde antivirüs motoruna sahip olması tercih sebebidir. Kullandığı antivirüs motoru bağımsız test kuruluşlarının en az biri tarafından teste tabi tutulmuş ve sonuçları yayınlanmış olmalıdır.

4.10. WAF ürününün antivirüs veritabanı üretici tarafından otomatik olarak güncellenmelidir.

4.11. WAF ürününün antivirüs koruması için 3th party ürünlerle entagrasyona gerek olmadan kendi üzerinde koruma sağlayabilmesi ve üreticinin yayınladığı antivirüs imza güncellemelerini otomatik olarak alabiliyor olması tercih sebebidir.

4.12. WAF ürünü dosya upload işlemlerinde dosya boyutuna göre kısıtlama sağlayabilmelidir.

4.13. WAF ürünü dosya upload işlemlerinde dosya tipine göre kısıtlama sağlayabilmelidir. Dosya tipine göre sağlanan kısıtlama sadece dosyanın uzantısına göre değil, metadata'sından dosyanın tipini anlayabilen mekanizmaya sahip olmalıdır.

4.14. WAF ürünü üzerinde korunacak uygulama bazında herhangi bir lisans limitasyonu bulunmamasi tercih sebebidir.

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

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

4.17. WAF ürünü, koruduğu uygulamanın önceden tanımlanmış dizinlerini öğrenip izleyebilmeli ve izinsiz değişiklik (Web Defacement) yapıldığında bunu farkederek raporlayabilmeli, ayarlanması durumunda otomatik olarak eski haline otomatik olarak geri dönebilmelidir.

4.18. WAF ürünü uygulama seviyesindeki DoS ataklarını anlayabilmeli ve engelleyebilmelidir.

4.19. WAF ürünü uygulama seviyesinde aşağıdaki DoS korumalarını sağlayabilmelidir;

- Src IP tabanlı HTTP Request limitasyonu
- Aynı http cookie ile TCP bağlantısı
- Aynı http cookie ile HTTP İsteği
- Kullanıcı için tamamen transparan davranan Challenge/Response mekanizması

4.20. WAF ürünü bot ve robot koruması kapsamında bilinen arama motorlarını ayırt edebilmeli ve kötü arama motorlarını ve robotları (scannerlar, crawlerlar, spiders) engelleyebilmelidir. Bu veritabanı manuel imza yazmaya gerek olmadan üretici tarafından güncellenmelidir.

4.21. WAF ürünü bilinen arama motorlarının uygulamayı indexlemesi için konfigürasyon yapmaya izin vermelidir. (Örn: Google izinli, Bing izinsiz gibi..)

4.22. WAF ürününün ADFS Proxy özelliği olmalıdır. Microsoft ADFS'i uygulama seviyeside analiz edebilmelidir.

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

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

4.25. WAF ürününün SYN Cookie özelliği olmalıdır.

4.26. WAF ürünü SAML desteklemelidir.

4.27. WAF ürününün FTP koruma özelliği olmalıdır. Bu koruma kapsamında FTP üzerinden gelecek komutların kontrolünü, içerisinden geçen dosyaların kontrolünü, bağlantıların coğrafi kontrolünü yapabilmelidir.

4.28. WAF ürünü FTP üzerinden geçecek dosyalar için antimalware ve sandbox koruması yapabilmelidir.

4.29. WAF ürünü FTP koruması kapsamında yine üreticiye ait istihbarat ağından faydalanabilmeli, IP Reputasyonu ile koruma sağlayabilmelidir.

4.30. WAF ürünü DOS, Brute Force tarzı saldırılara karşı belli threshold değerleri aşıldığında CAPTCHA kodu çıkarabilmelidir.

4.31. WAF ürünü gizli form alanlarına karşı koruma politikası yazmaya izin vermelidir.
4.32. WAF ürünü “XSS”, “SQL Injection”, “CSRF”, “Directory Traversal” , “Buffer Overflow”, “Remote File Inclusion”, “Command Injection”, “Virus Upload” ataklarına karşı koruma sağlamalıdır.
4.33. WAF ürünü üzerinde bulunan her bir imza gerektiğinde profil bazlı kapatılabilmeli yada imza bazında IP beyazlistesi uygulanabilmelidir.
4.34. WAF ürününün saldırı logundan kısayol ile beyazliste (exclusion) yazılabilmesi tercih sebebidir.
4.35. WAF ürünü “Klasör Listeleme”, “Sunucudan Dönen Hata Yanıtları” gibi bilgi sızıntısına yol açabilecek konfigürasyon hatalarına karşı maskeleme yapabilmelidir.
4.36. WAF ürününün Man-In-The-Browser koruması bulunmalıdır.
4.37. WAF ürünü URL encoding yapılmış saldırılara karşı URL decoding yapabilmeli ve atak paternini tespit edebilmelidir.
4.38. WAF ürünü birden fazla kez URL encoding yapılmış saldırıları ardışık (recursive) olarak decode edebilmeli ve atak paternini tespit edebilmelidir.
4.39. WAF ürünü HTTP RFC (7230-7236) ‘ye göre uyumluluk kontrolü sağlamalı, RFC uyumluluğu olmayan (malformed) HTTP isteklerini engelleyebilmelidir.
4.40. WAF ürünü bilinen ataklara karşı imza veritabanına sahip olmalı, bu veritabanı üretici tarafından rutin olarak güncellenmelidir.
4.41. WAF ürününün web trafiğini otomatik öğrenme ve öğrendiği trafiğe göre otomatik olarak koruma politikası oluşturabilme özelliği olmalıdır.
4.42. WAF ürünü SSL Offload yapabilmelidir.
4.43. WAF ürününün yüksek SSL işleme kapasitesi olan özel donanımlar üzerinde gerçekleştirmesi tercih sebebidir.
4.44. WAF ürününün “authentication offload” özelliği bulunmalıdır. İstemci sertifika doğrulama(PKI Auth.) ve Single sign-on yapabilmelidir.
4.45. WAF ürününün zafiyet tarama özelliği olmalıdır. Böylelikle OWASP Top-10 koruması ile birlikte PCI-DSS uyumluluğuna katkı sağlaması beklenmektedir.
4.46. WAF ürünü üzerinde otomatik öğrenilecek alanlar için özel tanım yapılabilmeli, böylelikle bu alanlarda öğrenmeye dahil edilebilmelidir.
4.47. WAF ürünü üzerinde uygulamaya ait login parametreleri (form fields) tanımlandığı durumda uygulamaya giriş yapan kullanıcı adlarını trafik ve atak loglarında ayrı ayrı gösterebilmelidir(User Tracking)
4.48. WAF ürünü Java Unicode decode edebilmeli ve parse ettiği protocol üzerinden koruma sağlayabilmelidir.
4.49. HTTPS şifrelemesi TLS1.0, TLS1.0 TLS1.2 ve TLS1.3 desteklemeli, gerektiğinde istenen şifreleme metodu kapatılabilmelidir.
4.50. HTTPS şifreleme için poodle, heartbleed gibi zafiyetlere karşı sıkılaştırılmış politikalar ile koruma sağlanmalıdır.
4.51. WAF ürünü TSL (European Union Trusted Service List) desteklemelidir. Böylelikle güvenilen hizmet sağlayıcılarının CA sertifikaları sistem üzerinde manuel güncellenebilmelidir. Bu sertifikalar sertifika doğrulamasında kullanılabilmelidir.
4.52. WAF ürünü aynı zamanda HTTP yük dengeleme özelliğine sahip olmalıdır.
4.53. WAF ürünü content routing desteklemelidir. Aynı VIP IP’ye gelen istekler URL, Path, Header, Src IP, Sertifika SNI ve HTTP/2 seviyesinde farklı sunucu ya da sunucu gruplarına yönlendirilebilmelidir.
4.54. WAF ürünü yük dengeleme yaparken aşağıdaki algoritmaları kullanabilmelidir;
- Round Robin
- Weighted Round Robin
- Least Connection

4.55. WAF ürünü yük dengeleme özellikleri içerisinde “Persistency” özelliğine sahip olmalıdır. Aşağıdaki persistency kabiliyetlerini sunabilmelidir;
- Persistent IP
- Persistent Cookie
- Insert Cookie
- ASP Session ID
- PHP Session ID
- JSP Session ID

4.56. WAF ürünü uygulamanın içerisinde kullanılan giriş alanlarından kullanıcı isimlerini okuyabilmeli ve hem trafik loglarında hem de saldırı loglarında ayrı bir alanda gösterebilmelidir. Böylelikle kuruma özel kullanıcıların tüm hareketlerinin izlenmesine olanak sağlayacaktır.

4.57. WAF ürünü HTTP/2.0 protokolünü doğrudan desteklemelidir. HTTP/2.0 uygulamalarda inspection yapabilmek için HTTP/1.1’e çevirmemelidir.

4.58. WAF ürününün SSL trafiği için “Elliptic Curve” cipher suite’leri özel donanımlar üzerinde offload edebilmesi tercih sebebidir.

4.59. WAF ürününün XML/SOAP desteği olmalıdır. XML Schema tanımı yapılabilmeli yada XML/SOAP özelinde parametre, uzunluk vs. konfigürasyonu sağlayabilmelidir.

4.60. WAF ürününün WSDL desteği olmalıdır.

4.61. WAF ürününün JSON desteği olmalıdır. JSON schema doğrulaması, parametre, uzunluk vs. kontrolleri sağlayabilmelidir.

4.62. WAF ürünü sistemler arası fortmatlanmış veri paylaşımı için kullanılan WEBSOCKET protokolü üzerinde koruma sağlayabilmelidir.

4.63. WAF Ürünü OpenAPI 3.0 desteği bulunmalıdır, doğrulama yapabilmelidir.

4.64. WAF ürünü API Gateway özelliğine sahip olmalıdır.

4.65. WAF ürünü backend sunucunun varsayılan ağ geçidi olarak kullanıldığı durumlarda internete doğru SNAT yapabilmelidir.

4.66. WAF ürünü http trafiğinde caching/compression desteklemelidir.

4.67. WAF ürünü GZIP ve BROTLI caching mekanizmalarını desteklemelidir.

4.68. WAF ürünü API koruması için json, xml/soap, openapi ve gRPC formatlarını desteklemelidir.

4.69. WAF ürünü geleneksel uygulama tabanlı öğrenime ek olarak yapay zeka teknolojisini kullanarak uygulama, bot ve API için ayrı ayrı makine tabanlı öğrenimi de desteklemelidir. Veri toplama, hesaplama, test etme ve korumaya geçme fazları kullanıcı müdahelesi olmadan otomatik yapılmalıdır. Bu işlem adaptif olarak kendini otomatik tekrarlayabilir olmalıdır.

4.70. İstenmesi durumunda WAF ürünü imza güncellemesi yaptığında yeni gelen tüm imzaları monitor modda devreye alabilecektir.

5. LOGLAMA & RAPORLAMA

5.1. WAF ürünü SIEM ürünleri ile Log entegrasyonu sağlayabilmelidir.
5.2. WAF ürünü uzak loglama yaparken SIEM formatlarından CEF ve LEEF formatlarını desteklemesi tercih sebebidir.
5.3. WAF ürünü tekrar edilebilir paket bilgisini de(HEX Body) loglarında tutabilmelidir.
5.4. WAF ürününün yönetim arayüzünde (GUI) saldırı logları açık bir şekilde görüntülenebilmeli, saldırı bilgisine ek olarak saldırı paterni renklendirilmiş olarak gösterilmelidir.
5.5. WAF ürününün yönetim arayüzünde (GUI) saldırı logları gruplanmış şekilde görüntülenebilmeli, böylelikle fazla sayıda oluşabilecek saldırı logları sonucunda sistem yöneticisine görsel kolaylık sağlamalıdır.
5.6. WAF ürünü yönetim arayüzünde(GUI) web erişim logları (Access Log) görüntülenebilmeli, bunun için ek yazılım yada donanıma ihtiyaç duyulmadan loglara rahatlıkla erişim sağlanmalıdır.
5.7. WAF ürününün kendi arayüzünden görülecek erişim logu detaylarında trafiğin yönlendirildiği sunucu, kaynak IP, hedef IP, erişilen hostname, url, http istek başlık bilgileri, http cevap başlık bilgileri, istek süresi, cevap süresi, http yanıt kodu(200, 404, 500 vs.) bilgileri mutlaka bulunmalıdır.
5.8. WAF ürünü saldırı logları içerisinde eğer mevcut ise saldırının CVE ID'sini yazmalıdır.
5.9. WAF ürünü saldırı logları içerisinde OWASP Top10 saldırı tiplerinden hangisine ait bir saldırı olduğunu gösterebilmelidir.
5.10. WAF ürünü üzerinden üretilen rapor müşteriye özel olarak müşteri adı, logo, sayfa alt başlığı, sayfa üst başlığı gibi objelerin düzenlenebilmesine olanak tanımalıdır, bunun için ek yazılım yada donanıma ihtiyaç duyulmamalıdır.
5.11. WAF ürünü en az PDF formatında rapor çıktısı üretebilmelidir.

5- ANALYZER LİSANSI (1 Adet)

1- Kurumumuzda çalışan 1 Adet Fortinet Analyzer VM Raporlama Sistemi için güncelleme servisleri satın alınacaktır.
2- Kurum bünyesinde bulunan 1 (bir) adet Fortinet Analyzer raporlama sisteminin garanti süresinin bitiminden itibaren en az 3 YIL yazılım üretici güncelleme paketi teklife dahil edilmelidir.
3- **1 Adet FAZ VM 25GB/gün** Güvenlik sistemi için alınacak güncelleme servislerinin aşağıdakileri içermesi gerekmektedir:
4- 3 Yıl Süreli Firmware/Yazılım güncelleme
5- 3 Yıl Süreli Üretici firmadan 24x7 e-mail destek
6- Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.
7- Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.
8- Önerilen kayıt yönetim sistemi geçmişe yönelik olarak raporlama yapabilme özelliğine sahip olacaktır. Örneğin bant genişliği kullanımı, uygulama denetimi, URL filtreleme ile ilgili istenen tarih aralıklarında raporlar üretebilecektir.
9- pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.
10- Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek kayıtların yedekliliği sağlayabilmelidir.
11- 3 Yıl Süreli Yazılım Garantisi

6- HİPER BÜTÜNLEŞİK SİSTEM (3 Node)

TEKNİK ŞARTNAME

1. İleri Bütünleşik Sistem Kümesi oluşturulması (3 adet)
Teknik Özellikler:

1.1. Teklif edilecek sistem üreticiler tarafından bu amaçla özel olarak üretilmiş, hesaplama ve depolama katmanlarının aynı fiziksel donanım üzerinde yer aldığı, tek ekrandan yönetilebildiği, otomatik yük dengeleme ve performans izleme özelliklerine sahip, yüksek erişilebilirlik fonksiyonları içeren ileri-bütünleşik sanallaştırma platformları olacaktır. Virtual SAN Ready Node veya benzeri yöntemlerle bir araya getirilmiş çözümler kabul edilmeyecektir.

1.2. Teklif edilecek sistem sanallaştırma ortamının kurulumu için gerekli tanımlamaların yapılacağı ekranlara sahip olacaktır. Sanallaştırma altyapısının kurulumu, sisteme yeni sunucu eklenmesi, ağ ve veri depolama katmanlarının yönetimi gibi fonksiyonlar otomatik olarak arayüzler üzerinden yapılabilecektir.

1.3. Teklif edilecek sistem her bir sistem kümesi içinde eşlenik Uç Noktalardan oluşmalı, bu Uç Noktaların üzerindeki fiziksel kaynakları her bir sistem kümesinin yönetim yazılımları aracılığıyla ortak bir havuz olarak yönetilmelidir.

1.4. Teklif edilecek sistem fiziksel sunucuların üzerindeki diskleri kullanarak ortak depolama alanı oluşturmalı ve sunucuların bu alanı ortak olarak kullanmalarını sağlamalıdır. Bu özellik için gerekli yazılımlar teklife eklenmelidir.

1.5. Teklif edilecek sistemi genişletmek için, sistemi kesintiye uğratmadan Uç Noktalar eklenebilmeli ve sistem büyütülebilmelidir.

1.6. Teklif edilecek sistemle farklı lokasyonlardaki sistem kümelerinin tek noktadan yönetimi mümkün olmalıdır. Tek noktadan yönetim için ek bir yazılım gerekiyorsa, ihtiyaç duyulabilecek tüm lisanslar eksiksiz olarak teklife eklenmeli, bu yönetim yazılımı her lokasyonu ayrı ayrı yönetebilecek şekilde lokasyonlara da kurulabilmelidir.

1.7. Teklif edilecek yönetim yazılımı, yönetimi altındaki tüm sistemlerin sağlık durumlarıyla ilgili bilgi ekranlarına sahip olmalı, bu ekranlar üzerinden veri depolama, işlemci ve bellek kullanımlarına dair bilgiler görüntülenebilmelidir.

1.8. Teklif edilecek sistemin veri sıkıştırma ve tekilleştirme özellikleri bulunmalıdır. Tekilleştirme ve sıkıştırma işlemleri için Uç Noktalar, üzerlerindeki Intel işlemcileri kullanacak, bu işlemler için kullanılacak maksimum işlemci kaynağı belirlenebilecektir. Maksimum işlemci kaynağının belirlenemediği (ayarlanamadığı) çözümlerde, her bir Uç Nokta için 2.2 maddesinde istenen fiziksel çekirdek miktarının en az %10 fazlası teklif edilmelidir.

1.9. Teklif edilecek sistemde tekilleştirme ve sıkıştırma işlemleri, veriler Uç Noktalardaki disklere yazılmadan önce yapılmalıdır. Veriler disklere yazıldıktan sonra arka planda veya cache amaçlı SSD disklere yazıldıktan sonra, kapasite amaçlı kullanılacak SSD disklere taşınırken küçültülüyorsa, bu çözümlerde ileri bütünleşik sistem kümesi için istenen net kapasitenin en az %10 fazlası teklif edilmelidir.

1.10. Teklif edilecek sistemin veri sıkıştırma fonksiyonu, kümelere yazılacak tüm veriler için aktif olmalı ve kapasite avantajı sağlamalıdır. Veri bloklarının sıkıştırılması için belli bir sıkıştırma oranının sağlanamadığı çözümlerde, ileri bütünleşik sistem kümesi için belirtilen net disk kapasitesinin en az %10 fazlası teklif edilmelidir.

1.11. Teklif edilecek Uç Noktalar arasında veri yedekliliği, verinin birden fazla kopyasını tutarak sağlanacak, sistem kümesinin net alan hesaplaması için Uç Noktalar arasında parite hesaplamasına dayalı metotlar kullanılmayacaktır.

1.12. Teklif edilecek sistem, her bir küme içinde aynı anda bir Uç Noktanın tamamen devre dışı kalmasını ve eş zamanlı olarak en az 1 Uç Nokta üzerindeki bir diskin daha arızalanmasını tolere etmelidir. Bu senaryoda veri kaybı olmayacağının garanti edileceği çözümler teklif edilmeli, net alan hesaplamaları bu yedeklilik seviyesi için yapılmalıdır.

1.13. Teklif edilecek sistemin üreticisi, sanal makinenin veri yazma isteğinin onaylanmadan önce küme içerisindeki en az iki farklı sunucuya yazım yapılacağını ve ani kesintilerde veri kaybı olmayacağını taahhüt edecektir.
1.14. Teklif edilecek sistem uzak sisteme replikasyon özelliklerini destekleyecektir. Bu özellik için ek yazılıma ihtiyaç duyan ürünler, üretici tarafından desteklenen ve çözüme entegre edilebilen üçüncü parti bir replikasyon çözümü ile teklif edilebilir. Bu özellik için ek lisanslama gerekiyorsa ihtiyaç duyulan sanal makine sayısı kadar veya tüm Uç Noktalar teklife dahil edilecektir. Uzak sistem replikasyonu ile en az 15 dakikalık geriye dönük kopyasının tutulabilmesi sağlanmalıdır.
1.15. Teklif edilecek sistemde kullanılması önerilen replikasyon yazılımları, geçmişe dönük replikaları bağımsız ve tam kopya şeklinde saklamalıdır. Önerilen çözümle orijinal sanal makinenin silinmesi durumunda dahi, yerel geçmişe dönük kopyalardan ya da uzak replikalardan geriye dönmek mümkün olmalıdır. Tanımlanan şekilde tam kopya özelliğini desteklemeyen replikasyon çözümleri değerlendirmeye alınmayacaktır. Saklanan tam kopya replikaların uygulama tutarlılığı olacak şekilde geri dönüşleri sağlanabilmelidir.
1.16. Teklif edilecek sistem, harici sistemlere de yedek alınabilmesini desteklemelidir.
1.17. Teklif edilecek replikasyon yazılımı, otomatize edilmiş felaket kurtarma orkestrasyonu desteğine sahip olmalıdır. Bu özelliğin kullanılabilmesi için gerekli ek bileşenler ve yapılandırılma gereksinimleri üretici tarafından kuruma aktarılmalıdır. Bu özellik için, kurumda halihazırda mevcut olan VMware Site Recovery Manager (SRM) lisansları kullanılacaktır. Farklı çözüm önerilerinin VMware Site Recovery Manager (SRM) fonksiyonlarını sağlaması ve sunacakları bütünleşik mimariyle kullanılabilmesi gerekmektedir.
1.18. Teklif edilecek sistemin yönetim arayüzü, sistemde oluşabilecek yazılım ve donanım hatalarını gösterecektir.
1.19. Teklif edilecek sistemin yazılım güncellemeleri, herhangi bir kesintiye sebep olmadan yapılabilmelidir.
1.20.Çözüm kapsamında ihtiyaç duyulacak tüm lisansların kurum adına temin edilmesi yüklenicinin sorumluluğundadır.
1.21. Mevcut sanallaştırma ortamındaki verilerin ve sanal sunucuların oluşturulacak sistem kümesine taşınması yüklenicinin sorumluluğunda olacak ve bu işlem uzman mühendisler tarafından tamamlanacaktır. Taşıma işlemi kurum ile birlikte mutabık kalınacak bir iş planı kapsamında yapılacaktır.
1.22. Teklif edilecek sistemin yönetim yazılımı, sanal sunucular için ayrı ayrı güç tüketimi politikaları uygulayıp, istenilmesi durumunda bir sunucunun belirlenmiş güç tüketimini aşmamasını sağlamalıdır.
1.23. Teklif edilecek sistemin kullanılacak sanallaştırma platformu ile uyumluluğu, ilgili üretici firmanın sertifikasyonu ile belgelenecektir.
1.24. Teklif edilecek sistemler tekilleştirme ya da sıkıştırma işlemleri için PCIe kartları gibi özel donanımlara ihtiyaç duyuyorsa üretici, arıza durumlarında anında destek olabilmek amacıyla kuruma özel yedek parça stoku tutacaktır.
1.25. Teklif edilecek sistem, aynı üreticinin D2D çözümüne herhangi bir yedekleme yazılımına ihtiyaç duymadan direk entegre olabilmeli, sistem yönetim arayüzünden yedekleme ve yedekten geri dönme işlemlerini yapılabilmelidir. Bu özelliği desteklemeyen çözümlerin yedek alabilmesi için gerekli olan yazılımlar ayrıca teklife eklenecektir.
1.26.Şartname kapsamında toplam en az 3 adet Uç Nokta teklif edilecektir. Teklif edilecek Uç Nokta sayısı 1.28 maddesinde yer alan tablodaki Sistem Kümesi Bazında Veri Yedeklilik Seviyesini sağlamıyorsa, gerekli yedeklilik seviyesini sağlayabilmek için yeterli miktarda Uç Nokta teklif edilmelidir. Teklif edilen tüm Uç Noktaların aynı cluster içinde işlemci, bellek, disk ve ağ kartı konfigürasyonları aynı olmalı, ileride değişebilecek ihtiyaçlar doğrultusunda sistem kümeleri arasında Uç Noktalar taşınabilmelidir.
1.27. Yukarıda belirtilen detaylar doğrultusunda temin edilecek Uç Noktalar kullanılarak, en az 1 adet ileri bütünleşik sistem kümesi oluşturulacaktır. En az 1 adet sistem kümesinin oluşturulabilmesi için gerekli tüm ek lisans ve donanımlar teklife dahil edilmelidir.

1.28.1 adet sistem kümesi oluşturulması için teklif edilmesi gereken minimum özellikler aşağıdaki tabloda yer almaktadır. Tablodaki değerler teklif edilebilecek en düşük değerler olup, kurum ihtiyaçları doğrultusunda şartnamede belirtilen gerekli ek bileşenler çözüme eklenmelidir.

Bütünleşik Sistem Kümesi	Uç Nokta Sayısı	Sistem Kümesi Bazında Veri Yedeklilik Seviyesi	Toplam Net Depolama Alanı Kapasitesi	Toplam CPU	Toplam Memory
1	**3**	Eşzamanlı bir uç nokta + 1 disk	**30 TB**	**96 p Core**	**3 TB**

2. Uç Nokta (Node) Temini ve Yerinde Çalışır Halde Kurulumu (3 adet)
Teknik Özellikler:
2.1. Teklif edilecek her bir Uç Nokta üzerinde en az 2 adet işlemci yuvası bulunacaktır.
2.2. Teklif edilecek her Uç Noktada, en az 2 (iki) adet Intel Scalable Xeon Gold serisi, en az 16 fiziksel çekirdekli ve en az 2.5 Ghz frekans hızında işlemci bulunacaktır.
2.3. Teklif edilecek her bir Uç Nokta üzerinde en az 1024GB DDR5 4800 Mhz hızında bellek bulunacaktır.
2.4. Gerekli disk adet ve kapasiteleri her bir üretici tarafından kendi çözümlerine en uygun şekilde belirlenecektir. Cache amacıyla kullanılacak SSD diskler ve boot diskleri sistemlerin optimum şekilde çalışabilmesi için üretici tarafında uygun görülen şekilde gerekli ve yeterli miktarda sunulmalıdır.
2.5. Uç Noktalar üzerinde ortak depolama havuzu için sadece SSD diskler kullanılacaktır.
2.6. Her Uç Nokta üzerinde en az 2 adet ayrı ayrı kartlar halinde dual portlu en az 10/25 Gbps hızında fiber ağ kartı bulunacaktır. Uç Noktaların omurga ağ bağdaştırıcılarına bağlanması için gerekli olan tüm kablo ve SFP modüller teklife dahil edilecektir.
2.7. Teklif edilecek Uç Noktalar üzerinde USB portları ve ekran bağlantı çıkışları bulunacaktır.
2.8. Her bir Uç Nokta üzerinde, hot-swap ve yedekli (redundant) yapıda soğutma fanları bulunacaktır.
2.9. Her bir Uç Nokta üzerinde, hot-swap ve yedekli (redundant) yapıda, güç kaynakları (Power Supply) bulunacaktır.

3. Genel Şartlar
3.1. Yüklenici firma, teklif ettiği ürünler için yetkili satıcı veya yetkili temsilci olduğunu gösteren belgelere sahip olmalı ve bu belgeleri ihale teklif zarfında sunmalıdır.
3.2. Yüklenici firmanın teklif edeceği bütün lisanslar her ürünün kendi üreticisinden sağlanan orijinal lisanslar olmalıdır.
3.3. Yüklenici firmanın teklif edeceği bütün ürünler, üretici firmanın garantisi kapsamında olmalıdır.
3.4. Yüklenici firma bahsi geçen bütün kurulumları hizmet kesintisine sebep olmaksızın yapmalı, gerekli hallerde Üniversite Yönetiminden hizmet kesintisi için yazılı izin almalıdır.
3.5. Yüklenici firma yılda en az 2 kez sistem sağlık kontrollerini yaparak varsa sistem hatalarını rapor etmelidir.
3.6. Yüklenici firma sözleşme süresi boyunca gerek duyulabilecek yapılandırma ve güncelleştirme hizmetleri için herhangi bir ek ücret talep etmeden gerekli çalışmaları yapmalıdır.
3.7. Yüklenici firma ihale konusu iş ile ilgili vereceği destek sürecince yapacağı işlerin muhtevasını ve bu çerçevede edindiği bilgileri gizli bir şekilde koruyacak, hiç kimseye hiçbir şekilde sözlü yâda yazılı bilgi paylaşımında bulunmayacaktır.

3.8. Yüklenici firma sözleşmenin imzalanmasından sonra Kişisel Verilerin Korunması Kanunu kapsamında Konya Karatay Üniversitesinin belirleyeceği gizlilik sözleşmesini imzalayacaktır. Gizlilik sözleşmesine aykırı bir durum ortaya çıkması durumunda, her türlü zararı tazmin edecektir.
3.9. Yüklenici firma tedarik edilen lisansları Konya Karatay Üniversitesi adına üretici firma sistemlerine kayıt ettirilecek, kullanıcı adı ve şifre doğrulaması ile giriş yapılarak bahsi geçen lisanslar görüntülenebilecektir.
3.10. Yüklenici firma kurulumu yapılacak sistemlere, sözleşme tarihinden itibaren üretici tarafından 5 yıl boyunca 7 gün 24 saat uzaktan ve en fazla bir sonraki iş günü içerisinde müdehale ile destek verileceğini taahhüt etmiş sayılacaktır.
3.11 .Bu teknik şartnamedeki maddelerde belirtilen özellikler asgari olup, şartnamedeki özellikleri sağlamak şartıyla daha üst özellikleri kapsayan ürünler teklif edilebilir.
3.12. Yüklenici firma ile birlikte belirlenecek veri taşıma planı doğrultusunda mevcut sunucuların tamamını taşıyıp ve sorunsuz bir şekilde çalıştırıldığını, üniversite ile teyitleştikten sonra ödemenin kalan %40 kısmını tahsil edecektir.

7- PROJEKSİYON (3 Adet)

1- Teklif edilecek ürün 3LCD Teknolojisi, RGB sıvı kristal deklanşör plmalıdır.
2- Teklif edilecek ürün 0,61 inç ile C2 Fine LCD panele sahip olmalıdır.
3- 4600 lümen 3200 lümen (tasarruf) renk ışık çıkışına sahip olmalıdır.
4- Full HD net bir görüntüye sahip olmalıdır.
5- 31 inçten 310 ince kadar ölçeklenebilir olmalıdır.
6- Ekonomik modda 30000 saate kadar kullanım ömrü olmalıdır.
7- 24 ay garanti, 36 ay lamba garantisi olmalıdır.