İZDENİZ
İZMİR DENİZ İŞLETMECİLİĞİ
NAKLİYE VE TURİZM TİCARET A.Ş.

İZMİR BÜYÜKŞEHİR BELEDİYESİ
İZDENİZ A.Ş.
TEKLİF İSTEME FORMU

DTN: 22DT65434
İlgili Birim: TEKNIK MÜD. - BİLGİ İŞLEM BİRİMİ

Teklif İsteme Tarihi: 28.01.2022

SIRA NO	SATIN ALINACAK MAL ve/veya HİZMETİN CİNSİ	Birim	Miktar	Toplam Tutarı (KDV Hariç)
1	GÜVENLİK DUVARI (FİREWALL) LİSANS 3 YILLIK	AD	1	

Yukarıda belirtilen Mal/Hizmetler teklif alma usulü ile satın alınacaktır/yaptırılacaktır. Bu işe alaka gösterdiğiniz takdirde aşağıdaki şartlar çerçevesinde tanzim edeceğiniz iş bu Teklif İsteme Mektubunu idaremiz satınalma birimine imzalı ve kaşeli olarak kapalı zarf içinde elden veya e-posta olarak gönderilmesini rica ederim.

Aydost GÜNDAY
Satınalma Müdürü

TEKLİF VERME VE SATINALMAYA İLİŞKİN HUSUSLAR:

1. Teklifinizi en geç **31.01.2022 saat 14:00'a kadar** İzmir Deniz İşletmeciliği Nakliye ve Turizm Tic. A.Ş. Satınalma Birimine gönderiniz.
   1.1. Adres: İzmir Marina Haydar Aliyev Bulvarı No.:4 Bahçelerarası Mahallesi Üçkuyular Balçova / İZMİR
   1.2. e-mail: satinalma@izdeniz.com.tr
   1.3. Tel : 0 232 320 00 35
2. Teklifinizi KDV hariç, **Birim Fiyat ve Toplam Bedel** olarak ve **TL** bazında veriniz. **Teklif mektubunun ve teknik şartnamenin her sayfasını kaşeleyip imzalayınız.** Varsa markasını mutlaka yazınız.
3. Teklif mektubunuzda teklif edilen mal ve/veya hizmetin toplam tutarı Kamu İhale Kanunu Doğrudan Temin Usulü ile alımda veya diğer ihale usulleriyle ihale edilmesine karar verilmesi halinde YAKLAŞIK MALİYET tespitinde değerlendirileceğinden SON FİYAT' ınızı yazınız. Doğrudan Temin Usulü ile alım yapılması halinde aşağıdaki şartlar geçerlidir.
4. **Şirketimiz E-Fatura mükellefidir. Siparişe konu mal/hizmetin faturası, E-Fatura mükellefi Yükleniciler tarafından 'TİCARİ FATURA' olarak düzenlenecektir.**
5. **01.01.2020 tarihinden itibaren E-Fatura mükellefi olmayan Yükleniciler, tarafımıza düzenleyecekleri vergiler dahil 5.000,00 TL ve üstü faturalarını E-Arşiv portalı üzerinden göndereceklerdir. Tarafımıza düzenlenen E-Arşiv faturalar fatura@izdeniz.com.tr e-mail adresine gönderilecektir.**
6. Teklif mektubunda vermiş olduğunuz fiyatlar Teknik Şartnamede aksine bir süre yoksa **30 (otuz)** gün süreyle geçerli olacaktır.
   6.1. Taahhüt edilen mal veya hizmet, Hasan Ali Yücel Bulvarı No:35 Bostanlı Vapur İskelesi Karşıyaka / İZMİR adresinde bulunan İZDENİZ A.Ş. Ambarına teslim edilecektir. Teslim süresinin bitiminde taahhüdün yerine getirilmemesi halinde geciken her gün için toplam tutarın (Teknik Şartnamede aksi bir oran yoksa) **%1 (yüzde bir)**'i oranında ceza uygulanır. **Ancak azami gecikme süresi 7 gün olup, gecikme süresinin 7 günü geçmesi halinde idare tek taraflı olarak alımdan vazgeçebilir.**
   6.2. Mal / hizmetin **TESLİM SÜRESİNİ MUTLAKA BELİRTİNİZ.** Teslim süresi 15 günü geçen alımlarda sözleşme imzalanacaktır. Yüklenici ile sözleşme imzalanması halinde, sözleşme tutarının **% 0,948 (binde 9,48)** oranında **sözleşme pulu** yüklenici tarafından sözleşmenin imzalanmasından itibaren yasal süresi içinde Vergi Dairesine yatırılacak ve alınacak belge fatura ile teslim edilecektir.
   6.3. Mal ve/veya hizmetin teslimi ve kabulünü müteakip ekli şartnamelerde aksine bir süre yoksa ödeme en geç **60 (Altmış)** gün içinde banka hesabına havale şeklinde olacaktır.
   6.4. **Teklif veren firmalar, yukarıdaki şartlarla birlikte, teknik şartname ve/veya numunedeki özellikleri aynen kabul etmiş sayılır.**
   6.5. İdare mal/hizmeti alıp almamakta veya bir kısmını almakta serbesttir.
7. **Teklif veren firmalar bağlı bulundukları Vergi Daireleri ve Vergi Numaralarını belirtecektir. Gerçek kişi olması halinde T.C. Kimlik No'sunu belirtecektir.** Tekliflerle ilgili ihtilaf halinde kurum kayıtları esas alınacaktır.
8. Teklif mektubunda teklif edilen bedel rakam ve yazı ile yazılmalı, üzerinde kazıntı silinti ve düzeltme bulunmamalıdır. Ad, Soyad ve Ticaret Unvanı yazılmak suretiyle yetkili kişiler tarafından imzalanmış ve kaşelenmiş olmalıdır.
9. Yüklenici 6183 sayılı kanunun 22/a maddesi gereği 5.000,00 (Beş Bin)TL'yi geçen tüm ödemelerde "Borcu Yoktur" belgesini ibraz edecektir.
10. İhale ilanlarımızı (www.izdeniz.com.tr) internet adresimizden takip edebilirsiniz.

Ek: Teknik Şartname (7 Sayfa)

TEKLİF VEREN KİŞİNİN/FİRMANIN:

Adı, Unvanı :
Vergi No :
Adres :
Tel/Faks :
Teklif Tarihi :

TEKNİK ŞARTNAME TARİHİ:	24.01.2022	
TEKNİK ŞARTNAME NUMARASI:		
TEKNİK ŞARTNAME KONTROL NUMARASI:	28.01.2022 10:01:59	

GÜVENLİK DUVARI (FİREWALL) LİSANS TEKNİK ŞARTNAMESİ	
TEKLİFLERİN VERİLECEĞİ ADRES, TELEFON VE FAKS NUMARASI:	
İDARENİN ADI	: İZMİR DENİZ İŞLETMECİLİĞİ NAKLİYE VE TURİZM TİC. A.Ş. (İZDENİZ)
İDARENİN ADRESİ	: İZMİR MARİNA-İZDENİZ HAYDAR ALİYEV BULVARI NO :4 BALÇOVA / İZMİR
İDARENİN TELEFONU	: 0(232) 320 00 35 FAKS: 0(232) 463 00 57
satinalma@izdeniz.com.tr	

1. İŞİN ADI

Güvenlik duvarı (firewall) lisans güncelleme işlemi

2. İŞİN KONUSU

İşletme bünyesinde kullanılmak üzere güvenlik duvarı lisans güncellemesi

3. TEMİNE İLİŞKİN İSTEK, ÖZELLİK VE ESASLAR

3.1. Genel Özellikler

3.1.1.Önerilecek çözüm en az aşağıdaki donanım özelliklerini karşılamalıdır.

- Donanım platformu 64 bit olmalıdır.
- En az 8 adet sabit 10/100/1000 mbps Ethernet portu olmalıdır.
- En az 8 adet 10/100/1000 mbps Ethernet portu eklenebilir olmalıdır.
- En az 64GB SSD diski olmalıdır.
- En az 2 adet USB portu olmalıdır.

3.1.2.Donanım aşağıda belirtilen ağ performans değerlerini karşılamalıdır.

- Eş zamanlı 3000000 (üç milyon) oturum sayısını desteklemelidir.
- Güvenlik duvarı paket filtre TCP throughput değeri 8000 (sekiz bin) mbps olarak ölçülmelidir.
- Web (URL) filtre throughput değeri 3000 (üç bin) mbps olarak ölçülmelidir.
- Anti-virüs throughput değeri 2400 (iki bin dört yüz) mbps olarak ölçülmelidir.

3.1.3.Ürün yerli sermayeli bir firma tarafından üretilmiş olmalıdır.

3.1.4.Güvenlik duvarı donanım tabanlı olmalıdır.

3.1.5.Güvenlik duvarı BSD tabanlı bir işletim sistemine sahip olmalıdır.

3.1.6.Güvenlik duvarı üzerinde iç ağa ait portlar bir switch gibi aynı ağ için kullanılabilmelidir.

3.1.7.Tek bir donanım/yazılım bütünü çözüm üzerinde şu bileşenler yer almalıdır:

- Ağ yönetim bileşenleri
- Paket filtre (firewall)
- Ağ geçidi anti-virüs
- Web (URL) filtre ve içerik filtre
- Atak tespit ve önleme sistemi (IDS/IPS)
- Uygulama filtre
- Hotspot ile misafir kullanıcı ağı yönetimi
- IPSec ile lokasyonlar arası (site-to-site) VPN
- SSL ile istemci-lokasyon arası (client-to-site) VPN
- Ağ trafiği kayıtlarını 5651 yasasına uyumlu şekilde tutabilme
- WAN (dış ağ bağlantısı) dengeleme ve yedekleme
- Active Directory entegrasyonu
- Raporlama

3.2. Ağ Yönetimi

3.2.1. Önerilecek çözümde DHCP sunucu yer almalıdır.
- Statik IP adresi tanımlanabilmelidir.
- Dinamik IP adresi dağıtabilmelidir.

3.2.2. DNS proxy yer almalıdır.

3.2.3. Statik DNS kaydı girebilme özelliği olmalıdır.

3.2.4. Yönetim arayüzünden aktif ağ taraması başlatılabilmeli, bulunan cihazlar statik IP adresi verilecek şekilde tek tuşla ilgili alana aktarılabilmelidir.

3.2.5. Yönetim arayüzünden ağdaki hangi cihazların en çok indirme ve yükleme yaptıkları, ne kadarlık trafik yarattıkları canlı olarak izlenebilmelidir.

3.3. Paket Filtre (Firewall)

3.3.1. Güvenlik duvarı durum korumalı (stateful) paket izleme yapmalıdır.

3.3.2. Güvenlik duvarında kaynak, hedef, servis, zaman bazlı kurallar tanımlanabilmelidir.

3.3.3. Güvenlik duvarında bant genişliği limitleme yapılabilmelidir.

3.3.4. Güvenlik duvarında statik, kaynak, hedef bazlı port yönlendirme yapılabilmelidir.

3.3.5. Güvenlik duvarında kural tabanlı yönlendirme (policy based routing) yapılabilmelidir.

3.3.6. Güvenlik duvarında Active Directory entegrasyonu olmalıdır.

3.3.7. Güvenlik duvarı kurallarında yükleme (upload) ve indirme (download) bant genişliği sınırlandırılması yapılabilmelidir.

3.3.8. Güvenlik duvarında adres dönüşümü (NAT) yapılabilmelidir.

3.3.9. Güvenlik duvarında SIP NAT yapılabilmelidir.

3.3.10. Güvenlik duvarında birden fazla dış ağ (WAN) bağlantı desteği olmalıdır.

3.3.11. Güvenlik duvarında bir arayüzde birden fazla dış IP adresi desteği olmalıdır.

3.3.12. Güvenlik duvarında VLAN desteği olmalıdır.

3.3.13. Güvenlik duvarında IP-MAC eşleştirme desteği olmalıdır.

3.3.14. Güvenlik duvarı, ağdaki mac adresi değişikliklerini takip ederek şu tespitleri yapabilmelidir:

3.3.15. IP çakışmasını (çakışan donanımların MAC adresini de listeleyerek)

3.3.16. Ağda yeni bir donanım ve yeni bir MAC adresi ile internete erişim yapılmakta olduğunu

3.3.17. Güvenlik duvarında köprüleme (bridge) desteği olmalıdır.

3.3.18. Güvenlik duvarında VoIP desteği olmalıdır.

3.3.19. Güvenlik duvarı içeride yapılandırılmış PPPoE istemcisi sağlamalıdır ve her PPPoE IP adresi değiştiğinde gerekli yapılandırmayı otomatik olarak güncelleştirecek kapasitede olmalıdır.

3.3.20. Güvenlik duvarında ülke bazlı engelleme özelliği bulunmalıdır. Ülkelerin IP adres blokları otomatik olarak çekilebilmeli ve güncellenmeli, elle yüklenmesi gerekmemelidir.

3.3.21. Hotspot kullanıcıları güvenlik duvarı kurallarına tek tek veya grup nesnesi olarak eklenebilmelidir.

3.4. Ağ Geçidi Anti-Virus

3.4.1. Anti-virüs sistemi, sisteme entegre web (URL) filtre ile beraber, web proxy ile seri olarak bağlı şekilde kullanabilmelidir.

3.4.2. Güvenlik duvarı, HTTP ve HTTPS trafiğindeki virüs ve kötü niyetli kodların imza tabanlı tespitini sağlamalıdır.

3.4.3. Güvenlik Duvarı imza veritabanını otomatik olarak her gün güncelleme kontrolü yapabilmeli, yeni imzaları otomatik olarak çekebilmelidir.

3.5. Web (URL) ve İçerik Filtreleme

3.5.1. Web (URL) filtreleme çözümü ürünle entegre olarak ürün üzerinde bulunmalıdır.

3.5.2. Kategori, kelime, dosya tipi bazında filtreleme yapılabilmelidir.

3.5.3. Yerel veritabanı ve Active Directory ile kullanıcı bazında kural yazılabilmelidir.

3.5.4. Web siteleri ve kategori bilgisi yerel olarak ürününün içinde saklanmalıdır.

3.5.5. İsteğe bağlı adres tanımlamaya dayalı URL'ler tanımlanabilmelidir.
3.5.6. Güvenlik duvarı ileti bloke etme sayfası özelleştirmesi yapılabilmelidir.
3.5.7. Güvenlik duvarı URL filtreleme farklı portlar üzerinden de yapılabilmelidir.
3.5.8. Güvenlik duvarı URL filtreleme HTTPS protokolü için istenirse de çalışabilmelidir.
3.5.9. Güvenlik duvarı URL filtreleme özelliği kayıt tutmalı ve IP adresi isteklerine, domain adına, URL'ye, web sitesi kategorisine göre raporlar verebilmelidir.
3.5.10. USOM (Ulusal Siber Olaylara Müdahale Merkezi) kara listeleriyle otomatik entegrasyon sağlanmalıdır.
3.5.11. Google, Youtube, Bing ve Yandex arama motorlarında güvenli arama (safe search) yapma özelliği bulunmalıdır.

3.6. IDS/IPS (Saldırı Tespiti ve Önleme)

3.6.1. Güvenlik duvarı saldırı tespit imzaları ile anomali tespiti yapabilmeli ve istendiğinde ilgili bağlantıları önleyebilmelidir. Sistem uyarı ve/veya engelleme moduyla çalıştırılabilmelidir.
3.6.2. Güvenlik duvarı IPS imzaları uzaktan otomatik olarak güncelenebilir olmalı, istenen kurallar arayüz üzerinden aktive edilebilmeldir.
3.6.3. En az 2500 IPS/IDS imzası olmalıdır.
3.6.4. Güvenlik duvarı ataklar için alarmlar üretebilmelidir.
3.6.5. Güvenlik duvarı geçmişe yönelik IPS raporlaması verebilmelidir.
3.6.6. Güvenlik duvarı saldırı imzalarıyla tespit edilen anormalliklere ait bağlantıları belirli bir süre otomatik olarak engelleyebilmelidir.
3.6.7. Bloklanan adreslerin listesi yönetim arayüzünde görülebilmelidir.

3.7. Uygulama Filtre

3.7.1. Uygulama filtre olarak ayrı bir bileşen yer almalıdır.
3.7.2. Uygulama filtre ile Layer7 (uygulama katmanı) düzeyinde kontrol sağlanmalı, imzası bulunan uygulamalar engellenebilmelidir.
3.7.3. Kategori ve uygulama bazında hazır kurallar olmalıdır.

3.8. Hotspot

3.8.1. Güvenlik duvarı üzerinde entegre olarak çalışan bir misafir ağ yönetimi (hotspot) bileşeni olmalıdır.
3.8.2. Misafir kullanıcının giriş yaptığı web ekranında Türkçe, İngilizce, Almanca, Rusça hazır dil desteği olmalıdır.
3.8.3. Kullanıcı giriş ekranı özelleştirilebilmelidir. Ekrandaki metinler ve renkler yönetim arayüzünden değiştirilebilmelidir. Ekrana logo eklenebilmelidir.
3.8.4. Kullanıcı giriş ekranına KVKK (Kişisel Verileri Koruma Kanunu) kapsamında aydınlatma metni eklenebilmelidir.
3.8.5. Yönetim arayüzünden kullanıcı giriş ekranının HTTP veya HTTPS olarak seçilebilmesi sağlanmalıdır.
3.8.6. Yönetim arayüzünden farklı diller eklenebilmelidir.
3.8.7. Kullanıcının web tarayıcısının diline göre giriş ekranının dili otomatik olarak belirlenebilmelidir.
3.8.8. Kullanıcı internete girme yetkisi aldığında yönetim arayüzünden belirlenebilen bir adrese yönlendirilebilmelidir.
3.8.9. Her kulanıcıya süre veya tarih bazlı zaman sınırı tanımlanabilmelidir.
3.8.10. Bir kullanıcı erişim şifresi, TC kimlik no ve SMS gibi aynı anda 3 farklı doğrulama yöntemi kullanılarak doğrulanabilmelidir.
3.8.11. Kullanıcının cihaz sayısı sınırlanabilmelidir.
3.8.12. İstenen kullanıcıların MAC adresleri girilerek hotspot oturumu açmadan hotspot tanımlanmış arayüzden internete bağlanmaları sağlanabilmelidir.
3.8.13. Kullanıcılara ilişkin raporlar alınabilmelidir.
3.8.14. Aşağıdaki yetkilendirme seçenekleri desteklenmelidir:

- Manuel
- Erişim şifresi ile

- TC kimlik no ile
- Yabanlı kimlik no ile
- SMS ile
- Otel veritabanı entegrasyonu ile

3.8.15. Hotspot yönetici paneli bulunmalıdır.

3.9. IPSec VPN

3.9.1. Güvenlik duvarı üzerinde entegre olarak çalışacak IPSec VPN bileşeni ile lokasyon-lokasyon (site-to-site) VPN bağlantısı sağlanabilmelidir.
3.9.2. IPSec VPN'de ön-paylaşımlı (pre-shared) anahtar ile yetkilendirmeye izin vermelidir.
3.9.3. IPSec VPN'de MD5 ve SHA-1 hash algoritmaları desteklenmelidir.
3.9.4. IPSec VPN'de 3DES, DES ve AES-128, AES-192, AES-256 şifreleme algoritmaları desteklenmelidir.
3.9.5. IPSec VPN'de Anahtar Grubu parametreleri desteklenmelidir.
3.9.6. IPSec VPN'de karşı tarafın koptuğunu tespit etme (dead-peer-detection) özelliği olmalıdır.
3.9.7. IPSec VPN'in NAT (Network Address Translation) arkasında çalışması desteklenmelidir.
3.9.8. IPSec VPN'de yerel ve hedef kimlik doğrulama işlemleri yapılabilmelidir.
3.9.9. IPSec VPN bağlantı kurma paketlerinin parçalanmış halde gönderimi desteklenmelidir.
3.9.10. IPSEc VPN'de yedekli çalışma özelliği desteklenmelidir.

3.10. SSL VPN

3.10.1. Güvenlik duvarı üzerinde entegre olarak çalışacak SSL VPN bileşeni ile istemci-lokasyon (client-to-site) VPN bağlantısı sağlanabilmelidir.
3.10.2. SSL VPN'de TCP ve UDP ile tünelleme yapılabilmelidir.
3.10.3. SSL VPN'de AES şifreleme algoritması desteklenmelidir.
3.10.4. SSL VPN'de yerel veritabanı ve Active Directory ile kullanıcı/grup yetkilendirmesi yapılabilmelidir.
3.10.5. SSL VPN'de verileri sıkıştırarak iletme seçeneği olmalıdır.
3.10.6. SSL VPN istemcilerine dinamik ve statik IP adresi verilebilmelidir.
3.10.7. SSL VPN sunucusu OpenVPN istemcileri ile tam uyumlu olmalıdır.
3.10.8. SSL VPN için ayrıca lisans gerekmemelidir.
3.10.9. SSL VPN için kullanıcı ve süre sınırı olmamalıdır.
3.10.10. SSL VPN'de kullanıcılara özel karakterli şifre verilebilmelidir.
3.10.11. SSL VPN'de kullanıcı login/logout bilgileri loglanmalıdır.
3.10.12 SSL VPN bağlantısı için kullanılacak sertifikalar yönetim arayüzünden indirilebilir olmalıdır.

3.11. WAN (Geniş Alan Ağı) Yük Dengeleme ve Yedekleme

3.11.1. Güvenlik duvarı, geniş alana birden fazla hat üzerinden otomatik olarak yük dengeleme ile çıkış sağlayabilmelidir.
3.11.2. Güvenlik duvarı tüm portlarından WAN yük dağılımını destekleyebilmelidir.
3.11.3. Her çıkış bağlantısı için, yükü yüzde (%) cinsinden belirterek bağlantı sayılarını istenen şekilde hatlar üzerinde dağıtabilmelidir.
3.11.4. Güvenlik duvarı, ağ geçidi durumunda bir değişim olursa uyarı mekanizmaları ile bildirim yapabilmelidir.
3.11.5. Güvenlik duvarına ait yük dağılımı yapılan hatların birinde kesinti olursa, tüm yükü diğer hat üzerine alabilmelidir.
3.11.6. Güvenlik duvarının USB portlarına Logo Siber Güvenlik tarafından desteklendiği belirtilen 3G/4G/4.5G USB modem bağlanabilmeli, bu modem WAN çıkışı olarak kullanılabilmeli, yedekleme ve yük paylaşımında kullanılabilmelidir.

3.12. Kayıtlar ve Raporlama

3.12.1. Raporlama çözümü, güvenlik duvarı üzerinde entegre olmalı ve ayrı bir kurulum gerektirmemelidir.
3.12.2. Raporlara güvenlik duvarı yönetim arayüzünden kolayca ulaşılabilmelidir.

3.12.3. Trafik geçiş ve engelleme, anti-virüs, saldırı tespiti ve önleme, web filtreleme, uygulama filtreleme, VPN, Hotspot, DHCP ve trafik raporları sağlanmalıdır.
3.12.4. Güvenlik duvarı en az bir Ethernet portu için bant genişliği kullanım istatistiklerini grafik olarak sunabilmelidir.
3.12.5. Güvenlik duvarı gerçek zamanlı anlık bant genişliği kullanımı bilgisini, kaynak ve hedef IP bazında verebilmelidir.
3.12.6. IP adreslerine göre indirme ve yükleme miktarları raporlanabilmelidir.
3.12.7. Kayıtlarda geçen IP adresleri, varsa tanımlı ağ nesnelerinin adlarıyla listelenmelidir.
3.12.8. Raporlarda zaman bazında filtreleme yapılabilmelidir.
3.12.9. Firewall cihazı üzerinden geçen paketler canlı olarak izlenebilmeli; arayüz, IP, port, protokol ve parametreler bazında bilgiler kullanılarak filtreleme gerçekleştirilebilmelidir. Aynı anda iki farklı ekran açılarak farklı arayüzlerdeki paketler birlikte izlenebilmelidir.
3.12.10. Raporlar CSV biçiminde dışarıya aktarabilmeli, bilgisayara indirilebilmelidir.
3.12.11. Kayıtlar yerel veya dış ağda bulunan Windows dosya paylaşım alanı veya Samba sunucu paylaşım alanı içinde tutulabilmelidir.
3.12.12. Kayıtlar FTP ve SFTP yöntemiyle dışarıya aktarılabilmelidir.
3.12.13. Kayıtlar 5651 yasasına uygun olarak tutulmalıdır.
3.12.14. Ürün içerisinde entegre bir 5651 çözümü olmalı, ayrı bir yazılım veya donanım ihtiyacı bulunmamalıdır.
3.12.15. Kayıtlara zaman damgası basabilmek için ürün üzerinde entegre olarak çalışan Kamu Sertifikasyon Merkezi (Tübitak), Turktrust ve E-imzaTR zaman damgası entegrasyonları olmalıdır.
3.12.16. Ürün, kendi üzerinde veya dışarıda tutulan kayıtlara zaman damgası basabilmelidir.
3.12.17. Kayıtlar yerel veya dış ağdaki bir Syslog sunucuya aktarılabilmelidir.
3.12.18. Ürün bir veya daha fazla Syslog sunucusundaki log verilerine zaman damgası basarak kendi üzerine kopyalayabilmelidir.

3.13. Mobil Rapor Uygulaması

3.13.1. Güvenlik duvarının IOS ve Android işletim sistemlerini destekleyen bir mobil raporlama uygulaması olmalıdır.
3.13.2. Bu uygulama içerisinde sınırsız sayıda berqnet cihaz için hesap tanımlanabilmeli ve her cihaz için aşağıdaki raporlar görülebilmelidir:
3.13.2.1. Temel web filtre ve trafik raporları
3.13.2.2. Kaynak kullanımı
3.13.2.3. Ağ kullanımı
3.13.2.4. Sistem ve servis bilgileri
3.13.2.5. Lisanslar
3.13.2.6. Uyarılar
3.13.3. Uygulama içerisinden cihazların yeniden başlatılması sağlanabilmelidir.
3.13.4. Uygulama içerisinde tanımlanmış cihazlar üzerinde oluşan uyarılar eş zamanlı olarak mobil rapor uygulamasında push bildirimi olarak görülmelidir.
3.13.5. Uygulama arayüzünün Türkçe ve İngilizce desteği olmalıdır.
3.13.6. Mobil uygulama kullanıcıları için berqnet cihaz üzerinde farklı yetki seviyelerine göre hesaplar tanımlanabilmelidir.
3.13.7. Uygulama içerisinde tanımlı cihaz hesapları dışarıya alınıp (export edilip) başka bir cihazda kurulu olan uygulamaya aktarılabilmelidir (import). IOS olan bir cihazdaki hesaplar Android olan bir cihazdaki uygulamaya aktarılabilmelidir.

3.14. Sistem Yönetimi

3.14.1. Güvenlik duvarı web-tabanlı (HTTPS) uzaktan yönetim özelliği sağlamalıdır.

3.14.2. Web arayüzü kullanımı kolay, gerekli yerlerde ayarlama sihirbazları sunan bir arayüz olmalıdır. Özellikle kural politikalarının hazırlanmasında, drag-drop (sürükle–bırak) teknolojileri kullanılıyor olmalıdır.

3.14.3. Sistemin tüm yapılandırması uzaktan web yönetim arayüzü üzerinden yapılabilmelidir. Konsol veya SSH üzerinden işletim sistemi üzerinde yapılandırma ihtiyacı hiçbir servis için bulunmamalıdır.

3.14.4. Konsola seri kablo üzerinden erişilebilmelidir. Konsol, sadece donanıma hatalı yapılandırma sonrasında erişilememe gibi durumlarda, çözüm amaçlı (şifre veya yapılandırma ayarlarını sıfırlama gibi) fonksiyonları içermelidir.

3.14.5. Konsol fonksiyonları, herhangi bir komut dili, işletim sistemi yapılandırma komutları olmadan, Türkçe bir arayüz ile sunulan menülerle yapılmalıdır. Herhangi bir özel CLI dili mecburiyeti kesinlikle gerektirmemelidir.

3.14.6. Güvenlik duvarı web arayüzü üzerinden, tüm işletim sistemi ve güvenlik politikaları yapılandırması yedeklenebilmeli, ve bu yedek geri yüklenerek tüm sistem geri alınabilmelidir.

3.14.7. Güvenlik duvarı iki farklı NTP sunucusundan zaman bilgisi alabilmelidir.

3.14.8. Güvenlik duvarı yönetim arayüzününün Türkçe ve İngilizce dil seçeneği olmalıdır.

3.14.9. Güvenlik duvarı bir uyarı sistemi barındırmalıdır. Bu sistem, hatalı şifre denemeleri, sistem anlık kaynak kullanımı (disk, işlemci) kritik seviyelerini, yük dağılımındaki ISP servislerindeki bir değişikliği, 5651 kayıt aktarım hatalarını yönetim arayüzünde bildirebilmelidir.

3.14.10. Sistem uyarıları istenen kişilere e-posta ile iletilebilmelidir.

3.14.11. Sistem yazılımı merkezi bir sunucudan otomatik veya manuel şekilde güncellenebilmelidir.

3.14.12. Güvenlik duvarı web arayüzü üzerinden, ağdaki hataların tespit edilebilmesine yönelik olarak aşağıdaki servisler sunulmalıdır:

- Ping atılabilmeli.
- Ethernet portlarını belirli bir adrese göre dinleyerek bağlantıları kontrol edilebilmeli.
- Traceroute ile donanımın ağ geçitlerini ve erişim hataları kontrol edilebilmeli.
- DNS sorgusu yapılabilmeli.
- Sistemin anlık gerçek zamanlı ağ tüketimi IP adresleri ve upload/download hızları ile raporlanabilmeli.

3.15. Lisanslama

3.15.1. Önerilecek lisanslarda kullanıcı sayısı sınırı olmamalıdır.

3.15.2. Lisanslama işlemi, cihaz arayüzünden lisans anahtarı girişi ile gerçekleştirilebilmelidir.

3.15.3. Üründe yer alan aşağıdaki özellikler, lisans süreleri sona erse bile çalışır halde olmalıdır. Bu bileşenlerin lisans süresi sona erdiğinde yazılım, imza, veritabanı gibi güncelleme işlemleri durdurulabilir fakat fonksiyonun çalışması durdurulmamalıdır:

- Paket filtre (firewall)
- Anti-virüs
- Atak tespit ve önleme sistemi (IDS/IPS)
- Uygulama filtre
- IPSec ile lokasyonlar arası (site-to-site) VPN
- SSL ile istemci-lokasyon arası (client-to-site) VPN
- WAN (dış ağ bağlantısı) dengeleme ve yedekleme
- Active Directory entegrasyonu

4. *NAKLİYE, TAŞIMA VE TESLİMATA İLİŞKİN ESASLAR*

Alıma konu malzeme teslim yeri teknik şartnamenin ilgili maddesinde belirtilen yerdir. Belirtilen bu yere teslimat yüklenici tarafından mesai saatleri içerisinde yapılacaktır. (Pazartesi – Cuma günleri arasında saat 08:00 ile 17:00 saatleri arasında)

5. *KABUL KRİTERLERİ*

İdarede mevcut kullanılan firewall lisansının kullanım süresinin 3 yıl süreyle yenilenmesine müteakip kabul komisyonu kabul sürecine başlar.

6. ÖDEME YERİ VE ŞARTLARIYLA AVANS VERİLİP VERİLMEYECEĞİ

(VERİLECEKSE ŞARTLARI VE MİKTARI İLE SÖZLEŞME KONUSU İŞLER İÇİN ÖDENECEKSE FİYAT FARKININ NE ŞEKİLDE ÖDENECEĞİ)

Bu iş için avans verilmeyecektir. İZDENİZ tarafından siparişe ait ödemeler, İZDENİZ A.Ş. Muhasebe ve Mali İşler Müdürlüğü tarafından yapılacaktır. Alım konusu olan firewall lisans yenileme işleminin teknik şartname ve alım dokümanlarına uygun şekilde 3 yıllık yenilenmesi koşuluyla, muayene ve kabul komisyonunca kabul raporu düzenlenir. Ödemelerin vadesi fatura tarihinden itibaren 30 (OTUZ) Gündür. İdaremizce ödemeler, her ayın ikinci CUMA günleri yapılır. Ödeme tarihi, fatura tarihinden itibaren 30 (otuz) gün sonraki ilk ödeme günüdür.

7. TESLİM YERİ

Teslim yeri " Hasan Ali Yücel Bulvarı No:35 Bostanlı Vapur İskelesi Karşıyaka - İZMİR" adresinde bulunan İZDENİZ A.Ş. ambarıdır.

8. İŞİN SÜRESİ

Firmaya siparişin verilmesine müteakip lisans süresi **10.02.2022** tarihinde başlayacak ve **10.02.2025** tarihinde sona erecektir. **Siparişin belirtilen güne kadar teslim edilmemesi durumunda, 7 (YEDİ) güne kadar toplam sipariş bedelinin %1 (YÜZDEBİR) oranında günlük gecikme cezası uygulanarak teslim alınabilir.**

9. İş bu teknik şartname, bu madde dâhil(9 (Dokuz)) ana madde olmak üzere 7 (Yedi) sayfadan ibaret olup tarafımızca hazırlanıp 24.01.2022 Tarihinde imza altına alınmıştır.

	HAZIRLAYAN	BİRİM SORUMLUSU	BİRİM MÜDÜRÜ
ADI SOYADI	Sercan Gül	Emre COBAN	A.KAĞAN DURMUŞOĞLU
GÖREVİ	Bilgi İşlem Personeli	Bilgi İşlem Sorumlusu	TEKNİK MÜDÜR