VERİ MERKEZİ HİZMET ALIM TEKNİK ŞARTNAMESİ

1. AMAÇ VE KAPSAM:

Doğuş Üniversitesi için veri merkezlerine erişilebilirlik ve sunucu barındırma hizmetlerinin sağlanması amaçlanmaktadır.

2. KULLANILAN TANIMLAR VE KISALTMALAR:

İdare :İhaleyi yapan kurum

İstekli :İhaleye teklif veren gerçek veya tüzel kişi

Yüklenici :İşi yüklenecek olan gerçek veya tüzel kişi

BT :Bilgi Teknolojileri

BT Altyapıları :Bilgi Teknolojileri tarafından sağlanan hizmetler için kullanılan donanım ve yazılım altyapı bileşenleri.

Erişim Altyapıları :İDARE tarafından ihtiyaç duyulacak erişim hizmetleri

Müdahale **:**Sorunun başlama zamanından itibaren, sorunun çözümüne ilişkin çalışmaların YÜKLENİCİ tarafından başlatılması ve İdare'ye süreçlerin raporlanması.

3. İŞİN TANIMI:

İDARE tarafından amaç kısmında belirtilen konulardaki hizmet ihtiyacı için aşağıdaki kapsamdaki iş kalemlerinde sözleşmede belirtilen tarihler arasında hizmet temin edilecektir:

S.Nu:	İş Kaleminin Adı ve Kısa Açıklaması	Birimi	Miktarı
1	Veri Merkezinden Kabin Sunucu Barındırma Hizmeti	Adet	1
2	IPV4 8 li Blok IP	Adet	5
3	1 GBPS INTERNET ERİŞİMİ	Gbit	1
4	1 GBPS DDOS PREMİUM GÜVENLİK PAKETİ	Gbit	1
5	3 KWA ELEKTRİK ENERJİSİ	Kwa	1

4. GENEL HÜKÜMLER:

4.1. YÜKLENİCİ, bu teknik şartnamede tarif edilen tüm hizmeti TÜRKİYE sınırları içinde olmak kaydıyla verebiliyor olmalıdır. İDARE ye ait veriler yurt dışına çıkarılmayacak ve yurt dışı kaynaklı hiçbir çözüm kabul edilmeyecektir.

4.2. Bulut hizmeti altyapısı, kurulum, taşınma ve devreye alma, işe başlama tarihinden itibaren en geç 90(doksan) takvim gününde mevcut sistemde kesintiye mahal vermeden ve veri kaybı yaşanmadan sağlanacaktır.

4.3. Erişim altyapısı, kurulum ve devreye alma, işe başlama tarihinden itibaren en geç 90(doksan) takvim gününde yüklenici tarafından sağlanacaktır.

4.4. İDARE'den kaynaklanacak gecikmeler yukarıdaki süreye eklenecektir.

4.5. 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında İDARE'nin YÜKLENİCİ bünyesinde barındıracağı sistemlerde bulunan verileri İDARE'nin yazılı izni olmaksızın veya yetkili mahkemelerce hukuki ve yazılı olarak talep edilmedikçe üçüncü taraflar ile paylaşamaz.

4.6. Veri merkezinde 7/24 tüm resmi ve dini bayramlarda dâhil olmak üzere kesintisiz olarak destek verilecektir.

4.7. Destek Hizmetleri kalifiye personel tarafından yürütülecektir.

5. VERİ MERKEZİ ÖZELLİKLERİ

5.1. Sanallaştırma hizmeti Tier 3 sertifikalı (Design-Facility-Operations) en az bir veri merkezinden sağlanabilmelidir.

5.2. Hizmet sağlayıcının en az bir lokasyonunda Veri Merkezlerinin Deprem Yönetmeliğine uygun sağlamlaştırma çalışmalarının yapılmış olması.

5.3. Veri merkezi için yıldırım tehlikesine karşı önlemler alınmış olacaktır.

5.4. Ortam sıcaklık değeri izleme, raporlama ve değer aşımları için alarm mekanizması bulunmalıdır.

5.5. Ortam nem değeri izleme, raporlama ve değer aşımları için alarm mekanizması bulunmalıdır.

5.6. Jeneratörlere ait yakıt depoları seviyesi standart süreç ya da otomasyon ile izlenmelidir.

5.7. Veri merkezi beyaz alan için minimum 8 saatte bir fiziksel ve görsel kontrol süreci bulunmalıdır.

5.8. Veri Merkezi binası hizmet sağlayıcıya ait olmalıdır.

5.9. İklimlendirme sistemi asgari N+1 yedekli olmalıdır.

5.10. Kullanılan klima sistemi hassas kontrollü olmalıdır.

5.11. İklimlendirme altyapısı optimum verimlilik için tasarlanmış olmalıdır. (Sıcak hava ya da soğuk havanın izolasyonu)

5.12. Veri merkezi içinde pozitif basınçlandırma için taze hava ve kullanılan havanın uzaklaştırılması için egzost sistemi olması gereklidir.

5.13. Kampüsü çevreleyen duvarlar üzerinde gece ve gündüz görüş kamera sistemi bulunacaktır. Kameralar 7x24 kayıt yeteneğine sahip olmalı ve kamera kayıtları asgari 1 yıl süre ile saklanmaktadır

5.14. Veri merkezi binasına girişte manyetik kartlı geçiş sistemi bulunmalıdır.

5.15. Yeşil enerji altyapısında çalışmalıdır.

a. Erişilebilirlik

i. Erişim hizmeti YÜKLENİCİ'nin kendi omurgasından sağlanacaktır.
ii. Erişim hizmeti asgari 3 farklı fiber optik güzergâhtan sağlayacaktır.
iii. YÜKLENİCİ, Veri merkezlerinde farklı operatörler için IP seviyesinde hizmet verebilecektir.

b. Enerji altyapısı

i. Veri merkezi orta gerilim enerjisi, iki farklı orta gerilim hücresinden sağlanacak ve asgari 2N yapıda olacaktır.
ii. Veri merkezi, iki farklı transformatör ‘den beslenecek. N+1 yapıda olacak ve aktif-aktif yapıda çalışacaktır.
iii. Veri merkezini besleyen jeneratörler asgari N+1 yedekliliğe sahip “continious” tip (sürekli çalışmaya uygun) olacaktır.
iv. Veri merkezini besleyen jeneratör tanklarında, veri merkezini en az 24 saat besleyecek yakıtı sürekli olarak bulunduracaktır.
v. Veri merkezi içerisindeki yükler asgari 2 farklı UPS grubu tarafından beslenmelidir. UPS grupları kendi içerisinde minimum N+ I yedekli olacaktır.
vi. Enerji altyapısı, kabinet başına en az 3 KW yedekli enerji sağlayabilecek şekilde olacaktır.
vii. UPS'ler farklı odalarda olacak ve bu odaların iklimlendirmesi asgari N+1 soğutma sistemi ile sağlanacaktır
viii. Her UPS grubu, tam yükte asgari 15 dakika back-up sağlayabilecek akü gruplarına sahip olacaktır.
ix. Her kabinette asgari 2 adet PDU olacak ve her PDU farklı UPS grupları tarafından beslenecektir.
x. Kabinetlerde bulunan PDU'lar (metered) uzaktan enerji tüketimi izlenebilecek şekilde olacaktır.

xi. Sistemin topraklama ölçümlerinin her yıl yapılıyor olacak ve EMO (Elektrik Mühendisleri Odası) belirttiği değerlerle olacaktır.
xii. Ölçüm yapılan cihazın kalibrasyon belgesi sunulacaktır.
xiii. Enerji ve veri kablolaması veri merkezi içerisinde birbirinden farklı rotalardan giderek kabinlerde sonlandırılacaktır.

c. İklimlendirme

i. İklimlendirme sistemi asgari N+1 yedekli olacaktır.
ii. Kullanılan klima sistemi hassas kontrollü olacaktır.
iii. İklimlendirme altyapısı optimum verimlilik için tasarlanmış olacaktır. (Sıcak hava ya da soğuk hava koridoru)
iv. Hizmet sağlayıcının en az bir Veri merkezi içinde pozitif basınçlandırma için taze hava ve kullanılan havanın uzaklaştırılması için egzoz sistemi olması gereklidir.

d. Fiziksel Güvenlik

i. Kampüs

1. Kampüs çevresinde. Kampüste veri merkezi bulunduğuna dair tabela, afiş gibi bilgilendirme sistemleri bulunmayacaktır.
2. Kampüsü çevreleyen yeterince yüksek, üzerinde dikenli tel bulunan beton duvarlar bulunacaktır.
3. Kampüsü çevreleyen duvarlar üzerinde gece ve gündüz görüş kamera sistemi bulunacaktır. Kameralar 7x24 kayıt yeteneğine sahip olmalı ve kamera kayıtları asgari 1 yıl süre ile saklanmaktadır
4. Kampüs girişinde, kampüse giren kişiler ve araçlar için bir güvenlik bulunacaktır.
5. Kampüse girişte bariyer sistemi bulunmalı, girişte 7x24 güvenlik sorgulaması yapılacaktır.
6. Hizmet sağlayıcının en az bir veri merkezinde Kampüse giren yabancı araçlar için bagaj kontrolü yapılacaktır.

ii. Veri Merkezi-Bina

1. Veri merkezi binasına girişte manyetik kartlı geçiş sistemi bulunacaktır.
2. Kartlı geçiş sistemi kayıtları yine sistem üzerinde en az 2 yıl geriye dönük saklanabilecektir.

3. Ziyaretçiler binaya X ray cihazından geçerek girebilecektir.
4. Ziyaretçiler bina girişinde Ziyaretçi kayıt sistemine kaydediyor olacaktır.
5. Ziyaretçi kayıt sistemi kayıtları en az 2 yıl geri dönük kayıtlar tutulacaktır. Hardcopy tutanaklar kullanılacaksa ise ek olarak taranmış halde softcopy olarak ta saklanacaktır.
6. Ziyaretçilere, ziyaretleri boyunca kullanacakları bir kart sağlanacak ve kartlar sadece ziyarete uygun alanlara, tanımlı süreler içerisinde giriş için yetkilendirilebilecektir.

iii. Veri Merkezi-Beyaz Alan

1. Beyaz alan girişinde bina girişindeki manyetik karta ek biometrik (örneğin retina tarama, parmak izi) bir güvenlik sistemi olacaktır.
2. Biometrik verilerin alınmasında ve yetki iptallerinde biometric verinin silinme işlemleri KVKK 'da belirtilen kurallar içinde yasal kanıt olarak silinme kayıtlarını verebilen sistemler kullanılıyor olacaktır.
3. Biometrik verisini paylaşmak istemeyen girişler için güvenli alternatif yöntemlerini sunulabiliyor olacaktır.
4. Beyaz alan girişinde aynı anda bir kişinin girişine imkân tanıyacak bir sistem kurulacaktır.
5. Beyaz alan malzeme giriş kapıları en az 47U boyundaki kabinlerin girişine uygun olacaktır.
6. Beyaz alana tüm giriş ve çıkış kayıtları tutulacaktır ve asgari 1 yıl süre ile saklanacaktır.
7. Beyaz alan içerisinde ziyaretçilere yapacakları çalışma süresince eşlik ediliyor olacaktır.
8. Beyaz alan kameralar ile izlenecek; kameralar kabinetlerin bulunduğu koridorları, her iki uçtan kabin ve arkalarını görecek şekilde olacaktır. Kamera görüntüleri en az 1 yıl geriye dönük erişilebilir biçimde sistem canlı sistem üzerinde saklanacaktır.

e. Yangın, Yangın Algılama ve Söndürme Sistemi

i. Veri merkezi ve kampüs çevresinde patlama ve yanına riski yüksek bir tesis bulunmayacaktır.

ii. Veri merkezi içerisinde ki tüm donanımlar aleve dayanıklı ve halojenden arındırılmış özellikli olacaktır.
iii. Veri merkezi binası için yangın algılama ve söndürme sistemi bulunacaktır.
iv. Veri merkezi beyaz alanı için gazlı söndürme sistemi ve hava örnekleme yangın algılama sistemi bulunacaktır.
v. Acil çıkış kapısı/kapıları olacaktır. Gerekli ışıklandırma ve yönlendirmeler içeride yapılmış olacaktır.
vi. Veri merkezinin bulunduğu bina ve beyaz alanlar için atanmış yangın sorumlulukları bulunacaktır.
vii. Veri merkezi bina ve kampüs için yangın tahliye planı bulunacaktır.
viii. YÜKLENİCİ, acil durum eylem planlarını ve yangın tahliye plan ve rutin test ve tatbikatlarını kurum ile paylaşacaktır. Görülen aksaklık ve sorunlar için en kısa sürede çözüm üretecektir.

f. Veri Merkezi Beyaz Alan Özellikleri

i. Veri merkezi beyaz alan içerisinde sıcak ve soğuk hava koridoru uygulaması yapılacaktır.
ii. Kabinlerin mekanik kilit anahtarlarının tutulacağı güvenli erişim yapılabilen anahtar dolapları bulunacaktır.
iii. Eğer beyaz alanda yükseltilmiş döşeme mevcutsa yüksekliği asgari 50 cm olacaktır
iv. Yükseltilmiş döşeme ayakları çapraz kuşaklar ya da çelik profil ile güçlendirilmiş olacaktır.
v. Yükseltilmiş döşeme, asma tavan arası asgari 3 metre olacaktır.
vi. Yükseltilmiş döşeme altı, epoksi veya tozumaz boya ile kaplanmış olacaktır.
vii. Enerji ve veri kablolama döşeme altında yapmış olması durumunda, havalandırmayı engellemeyecek bir yapı oluşturmuş olacaktır.
viii. Veri merkezi beyaz alan nem değeri %20-%80 arasında tutulacaktır
ix. Veri merkezi beyaz alan, soğuk hava koridoru ısı değeri ortalaması 18-27 derece arasında olacaktır.

g. İzleme Hizmetleri

i. Ortam sıcaklık değeri izleme, raporlama ve değer aşımları için alarm mekanizması bulunacaktır.

ii. Ortam nem değeri izleme, raporlama ve değer aşımları için alarm mekanizması bulunacaktır.
iii. Jeneratörlere ait yakıt depoları seviyesi standart süreç ya da otomasyon ile izlenecektir.
iv. Veri merkezi beyaz alan için fiziksel ve görsel kontrol süreci bulunacaktır.

h. Önleyici Bakım Hizmetleri

i. Tüm ekipmanların (Trafo, Jeneratör, UPS, Klima-iç ve Dış Üniteler. Elektrik Panoları, Yangın Algılama ve Söndürme Sistemleri, Geçiş Kontrol Sistemleri, Kapalı Devre TV Sistemleri, ...vb.) bakım anlaşmaları yapılmış ve güncel olacaktır.
ii. Tüm enerji ve altyapı ekipmanları kontrolü için veri merkezinde 7/24 personel bulundurulacak ve uygun sayılarda kontrol yapılacaktır.
iii. Sertifikalı ve periyodik bakımları yapılmış fiber ve bakır kablo test aletleri kullanılacaktır.

i. Su ve Sel Baskını

i. Sel baskının karşılık sağlanacak veri merkezinin, enerji odaları, UPS odası, akü odası ve beyaz alanı binanın bodrum katında bulunamayacaktır.
ii. Veri merkezi beyaz alanın bulunduğu binanın sel baskınına karşı koruması için kampüs çevresinde engel bulunacaktır.
iii. Veri merkezi beyaz alanının bulunduğu binada herhangi bir noktadan su sızıntısı, damlama ve akıntı (çatı dâhil) olmayacaktır.
iv. Veri merkezi beyaz alanın üzerinde ıslak zemin bulunmayacaktır.

6. SERTİFİKASYON

6.1. Hizmet sağlayıcı, sanallaştırma hizmetini sağladığı veri merkezlerinde aşağıdaki sertifikasyonları bulundurmalıdır ve Vmware Cloud Provider listesinde yer almalıdır.

i. ISO 27001 Bilgi Güvenliği Yönetim Sistemi
ii. ISO 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi
iii. ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi
iv. ISO 9001:2015 Kalite Yönetim Sistemi
v. ISO 10002 Müşteri Memnuniyeti Yönetim Sistemi
vi. ISO 50001 Enerji Yönetimi Sistemi ve İşleyiş Süreçleri
vii. ISO 27017 Bulut Güvenlik Sertifikası

viii. Hizmet sağlayıcı en az bir veri merkezinde TIER 3 Datacenter Design
ix. Hizmet sağlayıcı en az bir veri merkezinde TIER 3 Datacenter Facility
x. Hizmet sağlayıcı en az bir veri merkezinde TIER 3 Datacenter Operation
xi. Hizmet sağlayıcı en az bir veri merkezinde Leed Gold
xii. PCI DSS
xiii. Cloud Security Alliance (CSA) Star
xiv. Hizmet sağlayıcı en az bir veri merkezinde TS EN 50600 standartı sertifikası

7.1Kurumsal Siber Güvenlik Hizmetleri Özellikleri

7.1.1 L3 DDoS

7.1.1.1 Yüklenici temin edilecek olan internet devresin 7/24 gerçek zamanlı DDOS saldırılarından koruyacak hizmeti sağlayacaktır. Bu hizmet trafiğin gerçek zamanlı izlenmesine dayanmalıdır. Bu şekilde trafik üzerinde anormallikler anında tespit edilip sürekli koruma şeklinde gerçekleştirmelidir.

7.1.1.2 DDOS koruması kapsamında oluşan alarmları Kurumdaki yetkili kişilere eposta veya SMS olarak gönderilecektir.

7.1.1.3 Servis Sağlayıcı tarafından, Hizmet Alanın internet trafiği üzerinde "DDoS Atak Önleme Hizmeti" verilecektir. İnternet hattına DDoS saldırısı olması durumunda, saldırı trafiği, kullanıcı cihazlarına ulaşmadan önce önlenerek temizlenecektir.

7.1.1.4 Servis sağlayıcı tarafından hem marka hem de coğrafi yedekli yapı kurgulanmış olması tercih sebebidir.

7.1.1.5 Servis sağlayıcının altyapısı minimum 500 Gbps lik koruma kapasitesine sahip olmalıdır. 10 Tbps seviyesine kadar gelebilecek yüksek boyutlu atak durumunda YÜKLENİCİ Cloud DDoS hizmetini sunabiliyor olmalı ve gerektiğinde bu korumayı devreye alabilmelidir.

7.1.1.6 Servis sağlayıcı, HİZMET ALAN'ın internet devresinde 7/24 gerçek zamanlı DOS ve DDOS saldırılarından koruyacak hizmeti sağlayacaktır. Bu hizmet trafiğin gerçek zamanlı izlenmesine, ve trafiğin atak durumunda koruma cihazlarının üzerinden geçecek şekilde konfigüre edilmesine dayanmalıdır. Trafik üzerinde anomaliler trafiğin sürekli dinlenmesiyle tespit edilip otomatik koruma en geç 5 dakika içerisinde olacak şekilde otomatik koruma gerçekleştirilmelidir.

7.1.1.7 Servis sağlayıcı koruma ve internet hizmeti kapsamında sistemlerinde oluşan HİZMET ALAN ile ilgili hiçbir veriyi (istatistiki verisi, atak bilgisi, bant genişliği kullanım oranları) şahıs ya da diğer kurumlar ile paylaşmaz.

7.1.1.8 DDoS saldırı önleme hizmeti en az aşağıdaki saldırı tiplerine karşı koruma sağlayacaktır.

- ICMP Flood
- TCP Tabanlı Flood (SYN, FIN, RST, SYN ACK)
- UDP Flood
- Fragmentation ve Amplification tabanlı saldırılar
- İnternet Protokol RFC'lerine uymayan paketlerle yapılan saldırılar
- IP Spoofing Saldırıları
- Land Attack
- SIP Tabanlı Saldırılar (SIP Invite Flood)
- DNS Flood
- DNS Query Flood
- Malformed Protokol Tabanlı Saldırılar (Malformed DNS, Malformed SIP…)

7.1.1.9 Yüklenici tarafından sunulan hizmet aşağıda belirtilen koruma çözümlerini uygulayabilmelidir.

- RFC Tabanlı Invalid Paket Analizi
- IPV4/IPV6 Black/White Filter List
- IP Location Filter List
- Source Based Limitation
- Destination Based Limitation
- TCP SYN Authentication
- TCP Connection Limiting
- TCP Connection Control
- Payload Regular Expression Control
- DNS Authentication ve Rate Limiting
- HTTP Authentication ve Rate Limiting
- SIP Request Limiting

7.1.1.10 Normal trafik ile ilgili mevcut değerlerin sürekli hesaplanıp, bu değerleri aşan durumların atak olarak algılanarak korumanın başlaması sağlanmalıdır.

7.1.1.11 Koruma esnasında legal trafik ile atak trafiği birbirinden ayrıştırılabilmeli ve HİZMET ALAN'a temiz trafik sorunsuz şekilde iletilmelidir.

7.1.1.12 Atak anında ülke bazlı engelleme yapılabilmelidir.

7.1.1.13 Atak anında belirli ülkelerden gelen trafik limitlendirilmelidir.

7.1.1.14 Aylık veya HİZMET ALAN'ın talebine göre belirlenen zaman dilimi içerisinde atak raporları iletilmelidir.

7.1.1.15 HİZMET ALAN'ın talebine göre atak trafiğine dair detaylar (Kaynak ip , Kaynak Ülke , Packet Capture gibi) servis sağlayıcı tarafından paylaşılmalıdır.

7.1.1.16 DDoS Atak Önleme hizmeti içinde HİZMET ALAN'a özel trafik profilleri izlenerek ve karşılıklı çalışmalar sonucu oluşturulan ve periyodik güncellenen

koruma profilleri tanımlanabilmelidir. İhtiyaç durumunda birden fazla koruma profili oluşturarak farklı trafiklerin daha odaklı koruması sağlanabilmelidir.

7.1.2 L7 DDoS

7.1.2.2 Yüklenici temin edilecek olan internet devresinin 7/24 gerçek zamanlı Uygulama Seviyesi DDOS saldırılarından koruyacak hizmeti sağlamalıdır.

7.1.2.3 Uygulama katmanlı DDOS ataklarına karşı sunduğu hizmetinde korumanın aktif olması için atak tespit süresine ihtiyaç duyulmamalıdır. Bu hizmet ile devre trafiği sürekli olarak servis sağlayıcının sunduğu cihazlardan geçmeli ve koruma inline olarak sağlanmalıdır.

7.1.2.4 Yüklenici volumetrik olmayan uygulama seviyesindeki saldırılara karşı koruma sağlamalıdır.

7.1.2.5 Servis Sağlayıcı tarafından, Hizmet Alanın internet trafiği üzerinde "Uygulama katmanlı ataklara karşı DDOS atak önleme" hizmeti verilecektir. İnternet hattına DDoS saldırısı olması durumunda, saldırı trafiği, kullanıcı cihazlarına ulaşmadan önce önlenerek temizlenecektir.

7.1.2.6 Uygulama katmanlı ataklara karşı omurga seviyesinden koruma sağlanıp cihaz konumlandırılmaması tercih sebebidir.

7.1.2.7 Yüklenici firma devre kesintisi yaşanmaması adına topolojisinde otomatik BYPASS yapısı barındırmalıdır.

7.1.2.8 HİZMET ALAN'a internet ağına gelen saldırıları takip edebilmek için Yüklenici tarafından bir arayüz sağlanacaktır. Ayrıca saldırı sırasında e-posta ile bilgilendirme yapılmalıdır.

7.1.2.9 Yüklenici, koruma hizmetlerine dair tanımlama ve takip işlemlerini 7/24 esasına göre sağlayacaktır.

7.1.2.10 DDOS koruması kapsamında oluşan alarmları Kurumdaki yetkili kişilere eposta olarak gönderilecektir.

7.1.2.11 HİZMET ALAN, ilgili hizmet ile alakalı yüklenici tarafındaki sorumlulara 7/24 e-posta veya telefon yolu ile ulaşabilmelidir.

7.1.2.12 Servis sağlayıcı koruma ve internet hizmeti kapsamında sistemlerinde oluşan HİZMET ALAN ile ilgili hiçbir veriyi (istatistiki verisi, atak bilgisi, bant genişliği kullanım oranları) şahıs ya da diğer kurumlar ile paylaşmaz.

7.1.2.13 Inline DDoS saldırı önleme hizmeti en az aşağıdaki saldırı tiplerine karşı koruma sağlayacaktır.

- Slow Connection Atakları (Slowloris, Slowread, Slowpost)
- HTTP/HTTPS Flood (GET/POST)
- DNS Tabanlı Sorgu Atakları

- ANY DNS Atakları
- SIP Tabanlı Saldırılar (SIP Invite Flood)
- ICMP Flood
- TCP Tabanlı Flood (SYN, FIN, RST, SYN ACK)
- UDP Flood
- Fragmentation ve Amplification tabanlı saldırılar
- İnternet Protokol RFC'lerine uymayan paketlerle yapılan saldırılar
- IP Spoofing Saldırıları
- Land Attack
- DNS Flood
- Malformed Protokol Tabanlı Saldırılar (Malformed DNS, Malformed SIP…)

7.1.2.14 Yüklenici tarafından sunulan hizmet aşağıda belirtilen koruma çözümlerini uygulayabilmelidir.

- RFC Tabanlı Invalid Paket Analizi
- IPV4/IPV6 Black/White Filter List
- IP Location Filter List
- Source Based Limitation
- Destination Based Limitation
- TCP SYN Authentication
- Cookie Authentication
- Concurrent and New Connection Limiting
- DNS Authentication ve Rate Limiting
- HTTP Authentication ve Rate Limiting
- SIP Request Limiting

7.1.2.15 Normal trafik ile ilgili mevcut değerlerin sürekli hesaplanıp, bu değerleri aşan durumların atak olarak algılanarak korumanın başlaması sağlanmalıdır.

7.1.2.16 Koruma esnasında legal trafik ile atak trafiği birbirinden ayrıştırılabilmeli ve HİZMET ALAN'a temiz trafik sorunsuz şekilde iletilmelidir.

7.1.2.17 Atak anında ülke bazlı engelleme yapılabilmelidir.

7.1.2.18 Atak anında belirli ülkelerden gelen trafik limitlenebilmelidir.

7.1.2.19 Ülke bazlı engelleme ve limitleme ip-port bazlı yapılabilmelidir.

7.1.2.20 Aylık veya HİZMET ALAN'ın talebine göre belirlenen zaman dilimi içerisinde atak raporları iletilmelidir.

7.1.2.21 HİZMET ALAN'ın talebine göre atak trafiğine dair detaylar (Kaynak ip , Kaynak Ülke , Packet Capture gibi) servis sağlayıcı tarafından paylaşılabilmelidir.

7.1.2.22 DDoS Atak Önleme hizmeti içinde HİZMET ALAN'a özel trafik profilleri izlenerek ve karşılıklı çalışmalar sonucu oluşturulan ve periyodik güncellenen

koruma profilleri tanımlanabilmelidir. İhtiyaç durumunda birden fazla koruma profili oluşturarak farklı trafiklerin daha odaklı koruması sağlanabilmelidir.

7.1.2.23 Talep ettiği Veri Merkezi Erişim ve ME İnternet devrelerine L3-L4 hizmetine ek olarak herhangi fiziksel bir cihaz kullanmadan, YÜKLENİCİ omurga seviyesinde paylaşımlı olarak L7 DDOS hizmeti verebilmelidir.

7.1.2.24

7.1.3 DDoS Atak Önleme SLA

7.1.3.2 DDoS Atak Önleme hizmeti kapsamında olası DDoS saldırılarında Yüklenici alttaki tabloda verilen süreler içerisinde gerekli müdahaleleri yapacaktır.

		Basic Paket	
Öncelik	**Açıklama**	**İlk Müdahale***	**Çözüm**
Yüksek	Müşteri DDOS atağı nedeniyle erişim sorunu yaşamaktadır. Erişim ve paket kaybı sorunları Web servisi ve kurumun diğer servislerine DDoS veya Anti DDos kaynaklı erişim sorunu Inline DDoS koruma sorunları,	*30 Dk*	*3 Saat*
Orta	Kural ve konfigürasyon değişikliği talepleri, Cloud DDOS koruması problemi, Treshold güncelleme, cloud signalling talep ve arızaları	*1 saat*	*8 saat*
Düşük	Raporlamada ve arayüzde sorunlar yaşanmaktadır. Loglar görüntülenememktedir. Müşteri SSL VPN yapamamaktadır.	*4 saat*	*24 Saat*