İSTANBUL
TİCARET
ODASI
1882

İSTANBUL TİCARET ODASI

GÜVENLİK DUVARI İHALESİ TEKNİK ŞARTNAMESİ

2024

İÇİNDEKİLER

İSTANBUL TİCARET ODASI
GÜVENLİK DUVARI İHALESİ TEKNİK ŞARTNAMESİ

1. AMAÇ

İstanbul Ticaret Odası'nda ağ güvenliğini sağlamak amacıyla kullanılan mevcut güvenlik duvarı lisansının sona ermesi nedeniyle yeni bir güvenlik duvarı çözümü gerekmektedir. İlgili güvenlik duvarı çözümü, kurumun bilgi güvenliği gereksinimlerini karşılayacak, siber tehditlere karşı etkin koruma sağlayacak ve performans ile ölçeklenebilirlik açısından kurumsal ihtiyaçlara uygun olmalıdır. Temin edilecek güvenlik duvarı cihazının ileri düzey tehdit önleme, güvenli segmentasyon, SD-WAN entegrasyonu ve bulut tabanlı hizmetlerle uyumlu olması beklenmektedir.

2. GÜVENLİK DUVARI İÇİN GENEL ŞARTLAR

2.1. Kurum ortamında kullanılmak üzere 2 adet donanım ve yazılım bütünü (appliance) "Güvenlik Duvarı Sistemi" teklif edilecektir. İleride gerekli olması durumunda High-Availability için Active-Active ve Active-Passive olarak çalışmayı desteklemelidir. Active-Active çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer sistem tüm fonksiyonları üstlenerek, el ile müdahaleye gerek kalmadan çalışmaya devam edebilmelidir.

2.2. Lisanslar ve donanımların isteri **5** yıl olacaktır.

2.3. Yüklenici şartname maddelerini tek tek cevaplayacaktır.

2.4. Teklif edilecek ürün, aşağıda belirtilen özelliklerine asgari olarak sahip olmalıdır, bu özellikler için bir lisans gerekiyorsa lisans ücretleri ayrıca teklif edilmelidir.

- **2.4.1.** Güvenlik Duvarı (Firewall)
- **2.4.2.** IPSec VPN Sonlandırma Sistemi
- **2.4.3.** SSL VPN Sonlandırma Sistemi
- **2.4.4.** Saldırı Tespit ve Engelleme Sistemi (IPS)
- **2.4.5.** Uygulama Tanıma Kontrol (Application Control) Sistemi
- **2.4.6.** Virüs/Zararlı İçerik Kontrolü
- **2.4.7.** URL Filtreleme yeteneği ve proxy entegrasyonu
- **2.4.8.** HTTPS Tarama (SSL Inspection)
- **2.4.9.** Detaylı Bant Genişliği Yönetimi (QoS)
- **2.4.10.** SD-WAN (Software-Defined Wide Area Networking – Yazılım Tabanlı Geniş Alan Ağı)

2.5. Teklif edilen güvenlik sistemi içerisinde her bir donanım, en az UDP 1518 Byte paketler ile en az **50 Gbps** firewall 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.

2.6. Ürün, en az **27 Gbps** yeni nesil firewall (NGFW/IPS) performans (throughput) değerine sahip olmalıdır. Bu değer RFC standartlarında ölçülmüş lab değeri olmamalı, gerçek yaşam (min HTTP 64KB) değeri olmalıdır.

2.7. Ürün, en az **25 Gbps** Threat Protection performans (throughput) değerine sahip olmalıdır.

2.8. Aynı anda en az **6.4 Milyon** eş oturumu desteklemeli ve saniyede en az **360 bin** yeni oturum açabilme performansına sahip olmalıdır.

2.9. Çözüme ait özelliklerin ve kapasitelerin tek bir cihaz içinde sağlanması zorunludur.

2.10. Teklif edilecek donanım yedekli güç kaynağına (Redundant Power Supply) sahip olmalıdır.

2.11. Teklif edilecek çözüm üzerinde yerel storage diski olmalıdır.

2.12. Güvenlik Duvarı Sistemi en az **28 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.

2.13. Güvenlik Duvarı Sistemi en az **12 Gbps** SSL inspection throughput değerine sahip olmalıdır. Bu performans değeri IPS açık iken HTTP trafiğinin şifrelemesi ile elde edilmelidir. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

2.14. Sistem Network Arayüz'lerin herbiri; LAN, WAN, DMZ veya kullanıcı tarafından kuralları belirlenen bir segment olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve sistemin Network Arayüzleri üzerinde VLAN arayüzleri de tanımlanabilmelidir.

2.15. Ürün, aynı anda **6 x GE RJ45 Port**, en az **10 x 10GE/GE SFP+/SFP** sahip olmalıdır. İlgili portlar 1 Gbps bakır, 1 Gbps SX/LX fiber ve 10 Gbps SR/LR fiber GBIC modüllerini desteklemelidir. Cihaz ile birlikte en az 10 adet 10 Gbps SR ya da LR fiber GBIC verilmelidir. Ürün **40 veya 100 Gigabit Fiber (QSFP+)** interface desteği olmalıdır.

2.16. Önerilecek çözüm en az FIPS, EAL-4+, ICSA sertifikalarına sahip olmalıdır.

2.17. Teklif edilecek güvenlik duvarı ürünleri ve "2022-2023 Gartner Magic Quadrant for Enterprise Network Firewalls" raporunda "Leaders" kategorisinde yer alması tercih sebebidir.

2.18. En az Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, SMTP, SSH, NBT, SMB, MSRPC, POP3, SIP, TFTP, HTTPS (SSL/TLS), GRE, IP-in-IP, IPv6 encapsulation protokolleri için full normalization desteklenmelidir.

2.19. IDS/IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. TCP ve UDP protokolleri için el ile imza tanımlamaya imkan tanımalı, bunun için regex veya snort temelinde yöntemler kullanılabilmelidir.

2.20. Microsoft AD ile transparent olarak kimlik doğrulama yapmaya imkan tanımalıdır. Bunun için kullanıcı sistemlerine herhangi bir ajan kurmaya gerek kalmamalıdır. Multi Domain desteklenmelidir.

2.21. Kullanıcı kimlik doğrulama için web portal yöntemi desteklenmeli, bunun için RADIUS ve TACACS+ kullanılabilmelidir.

2.22. HTTPS ve Quic protokolü desteklenmeli ve HTTPS için deep packet inspection yapabilmelidir.

2.23. Çözüm bloklama için connection reset, blacklisting, html response, html redirect gibi yöntemleri kullanabilmelidir.

2.24. Çözüm, DOS saldırılarına karşı koruma sağlayabilmelidir.

2.25. Çözüm, Malware tarama özelliğine sahip olmalıdır. Üzerinden geçen HTTP, HTTPS, SMTP, POP-3 ve IMAP trafiklerini tarayarak virüsleri engelleyebilmelidir. Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Firewall Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virus imzalarını otomatik olarak güncelleyebilmelidir.

2.26. Sistem Kural tabanlı trafik biçimlendirme, Bant Genişliği kontrolu ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.

2.27. Çözümün IPv6 desteği tam olmalı, IPv4 ve IPv6 için NAT, Static NAT, Source NAT with Port Address Translation (PAT), Destination NAT with PAT desteklemelidir.

2.28. Static Routing olarak; IPv4 ve IPv6 Static Routes, Policy-Based Routing, Static Multicast Routing, Dinamik Routing olarak; IGMP proxy, RIP, OSPF, BGP desteklenmelidir.

2.29. Çözüm en az EtherChannel 802.1ad ve support 802.1q VLAN Tagging desteklemelidir.

2.30. BGP ve OSPF gibi protokollere gerek kalmadan 2 veya daha çok ISP link için load balancing desteklenmelidir. Linkler arasında en hızlı olan tespit edilip o link öncelikli seçilebilmelidir. Uzak ofisler için yedekli linkler üzerinden VPN load balancing desteklenmelidir.

2.31. Cluster mimaride Authenticated bağlantılar için statefull failover desteklenmelidir.

2.32. İki veya daha çok web server için load balancing desteklenmelidir. Ping veya özel ajan yolu ile sağlık kontrolüne imkân tanımalıdır.

2.33. AES-128/AES-256/DES/3DES kriptografik algoritmalar ve MD5/SHA-1/SHA-256 digest algoritmaları desteklenmelidir. Diffie Helman için; DH group 1, 2, 5, 14, 19, 20, 21 desteklenmelidir.

2.34. Sistemin üzerinde unlimited IPSEC VPN desteği olması tercih sebebidir, unlimited lisans verilemediği durumda en az **200 (iki yüz)** kullanıcı IPSEC VPN yazılımı ile eş zamanlı olarak VPN tünel kurabilmeli ve belirlenen sistemlere erişebilmelidir.

2.35. Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, Firewall Sistemi ile bütünleşik olarak çalışacak IPSEC VPN Client ve SSL VPN Gateway özelliği bulunmalıdır.

2.36. SSL VPN bağlantılar üzerinden güvenli olarak erişilen kurum kaynaklarında web tabanlı uygulamaların yanında özel herhangi bir uygulama da çalıştırılabilmelidir.

2.37. Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella, ve benzeri) ve Web Uygulamaları gibi tanımlı en az 2.500 adet uygulamaya ait trafiği kullanılan port'tan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir.

2.38. Sistemin Sanal Firewall desteği tercih sebebidir. Sistem üzerinde ki fiziki ve sanal arayüzler Sanal Firewall'lararasında paylaştırılarak yönetimleri ve kuralları birbirinden bağımsız sanal firewall'lartanımlanabilmelidir. Sistemle birlikte, en az 2 adet sanal Firewall sağlayacak lisanslar teklife dahil edilecektir. Donanım içerisinde sanal firewalllar stabil değil ise ayrı 2 adet donanım , Her biri en az 1gbit Threat Protection performans (throughput) değerine sahip olmalıdır. 5 yıl tüm blade lisansları ile birlikte teklife dahil edilmelidir.

2.39. Kimlik doğrulama için en az; RSA, DSS, ECDSA signatures with X.509 certificates, pre-shared keys, hybrid, XAUTH, EAP desteklenmelidir.

2.40. Ürün üzerinde detayları aşağıda iletilen URL Filtreleme özelliği bulunmalıdır.

2.40.1. URL filtreleme veri tabanında en az 250 milyon web adresi tanımlı olmalıdır.

2.40.2. En az 80 farklı kategori tanımı olmalıdır.

2.40.3. Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk url adresi, regex ve wildcard formatında tanımlı adreslere erişime izin verebilmeli veya engelleme yapabilmelidir.

2.40.4. USOM gibi harici karaliste kaynakları spesifik kategori olarak eklenebilmeli ve otomatik olarak güncellenebilmelidir.

2.40.5. Sadece domain bazında değil, erişilen ip bazında da kontrol yapabilmelidir.

2.40.6. URL filtreleme uyarı ekranı özelleştirilebilmelidir.

2.40.7. Ürünün, URL filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.

2.41. Ürün üzerinde detayları aşağıda belirtilen zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır.

2.41.1. Ürün, aşağıda belirtilen protokoller aracılığıyla yapılan malware trafiklerini tespit edip engelleyebilmelidir.

- HTTP(S),
- FTP,
- POP3,
- IMAP,
- SMTP,

2.41.2. Ürün, yukarıda belirtilen protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir.

2.41.3. AntiMalware sistemi Internet üzerinden virüs imzalarını otomatik olarak güncellenebilmelidir.

2.41.4. Sadece internet trafiğinde değil, istenirse lokal network erişimlerinde de AntiMalware kontrolü yapılabilmelidir.

2.41.5. AntiMalware sistemi, akıllı telefonlara yönelik mobil malware'leri tespit edebilme ve engelleme yeteneğine sahip olmalıdır.

2.41.6. Arşiv dosyalarının detay analizini yapabilmeli ve bozuk (corrupted), şifreli (encrypted), iç içe geçirilmiş (nested) arşiv dosyaları engellenebilmelidir.

2.42. Ürünün, güncel saldırıların engellenmesi amacıyla aşağıda detayları belirtilen atak engelleme (IPS) özelliği olmalıdır.

2.42.1. IPS sistemi aşağıda belirtilen saldırı tiplerini engelleyebilmelidir.
- Trafik Anomaly
- Protocol Anomaly
- Oran (rate) bazlı saldırılar (brute force gibi)
- Sızma temelli (evasive) saldırılar

2.42.2. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak da yapılabilmelidir.

2.42.3. Her bir IPS imzası için aşağıdaki aksiyonlar alınabilmelidir.
- İzin ver (pass)
- İzin ver ve olay kaydı al (monitor)
- Payload bilgisi ile log tut
- Paketi düşür

2.42.4. Tanımlı saldırı tiplerine göre saldırı yapan ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

2.42.5. Veritabanında yer alan imzalar aşağıdaki tanımlara göre filtrelenebilmelidir.
- Kullanılan uygulamaya göre (IIS, Oracle, SQL, Apache gibi)
- İşletim sistemine göre (Windows, Linux, Solaris gibi)
- Protokole göre (HTTP, HTTPS, FTP, DNS gibi)
- Risk seviyesine göre (Kritik, Yüksek Risk, Orta Risk, Düşük Risk gibi)
- Hedef işletim sistemine göre (client ve/veya server)

2.42.6. IPS sistemi aşağıda belirtilen detaylı sızma tekniklerine karşı koruma sağlayabilmelidir.
- IP Packet Fragmentation,
- TCP Stream Fragmentation
- TCP Stream Segmentation,
- RPC Fragmentation,
- URL Obfuscation,

2.42.7. Teklif edilen sistem, Botnet aktivitelerini imza tabanlı olarak tespit edebilmeli ve engelleyebilmelidir.

2.42.8. Teklif edilen sistem, Botnet C&C adreslerine doğru yapılan tüm trafikleri adres tabanlı tespit edebilmeli ve engelleyebilmelidir.

2.42.9. IPS imzası özelinde kaynak ve hedef adres bilgisine dayalı istisna adresler (exception) tanımlanabilmelidir.

2.42.10. Ürün, IPS loglarında saldırının yönünü gösterebilmelidir

2.43. Ürün üzerinde detayları aşağıda belirtilen uygulama kontrol özelliği bulunmalıdır.

2.43.1. Ürünün uygulama kütüphanesinde en az 2500 (ikibinbeşyüz) adet uygulama yer almalıdır.

2.43.2. Uygulama kütüphanesinde yer alan tüm uygulamalar aşağıda belirtilen parametrelere göre kategorize edilmiş olmalıdır.

- Uygulama davranışına göre (botnet, tünelleme amaçlı, bulut uygulaması, bandwith tüketim odaklı, sızma amaçlı gibi),
- Risk seviyesine göre,
- Kullanılan protokole göre (HTTP, DNS, FTP, SIP, H323 gibi),
- Üreticiye göre (Google, Microsoft, Apple gibi)

2.43.3. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir, sistem yöneticileri tarafında istenirse manuel olarak da güncellenebilir olmalıdır.

2.43.4. Ürün, yöneticileri tarafından özel uygulama imzaları tanımlamaya izin vermelidir.

2.43.5. Hedef port için protokol tanımı yapılabilmeli, bu sayede ilgili port üzerinden farklı protokol trafiği engellenebilmelidir (örneğin 80 portu üzerinden sadece HTTP trafiği, 53 portu üzerinden sadece DNS protokol trafiği yapılabilsin gibi).

2.44. Ürünün, aşağıda detayları belirtilen SD-WAN özelliği olmalıdır.

- Ürün, birden fazla geniş alan ağı (WAN) bağlantısının trafik paylaşımı amacıyla aktif/aktif mimaride kullanımını desteklemelidir.
- Birden fazla WAN bağlantısı tek bir sanal hat (virtual interface) gibi tanımlanabilmeli ve bu sanal hatta doğru kural (policy) ve rota (route) yazılabilmelidir.
- SD-WAN hatlarının bağlantı kalitesi takip edilebilmelidir.
- Kuralda tanımlı trafiğin spesifik olarak belirli bir hattan çıkarılması,
- Uygulama bazında spesifik SD-WAN kuralları tanımlanabilmelidir. Bu sayede örneğin Youtube gibi spesifik uygulama trafiklerinin spesifik hat üzerinden yönlendirilmesi sağlanabilmelidir.

2.45. Sistemlerin; Firewall, VPN, IDS/IPS fonksiyonlarının her biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Kurumsal Ağ Güvenlik Sisteminin 5 yıl süre ile Yazılım/Firmware güncellemelerini ve en az 5 yıl süre icin,IDS/IPS,SSL VPN, IPSec VPN , SDWAN, URL Filtering, Uygulama Kontrolu, AntiVirus güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir ve servis ve güncellemeler bu süre boyunca sağlanmalıdır.

3. YÖNETİM / LOG / RAPORLAMA SİSTEMİ

3.1. Güvenlik Duvarı Sistemlerini yönetim sistemleri yazılım olarak Windows ya da Linux işletim sistemleri üzerinde çalışabilmelidir. Fiziksel ya da sanal sunucular üzerinde çalışabilmelidir. Sunucular kurum tarafından sağlanacaktır.

3.2. Yönetim sistemleri aynı zamanda log sunucu olarakta çalışabilmeli, istenmesi durumunda log sunucusu ayrı bir sunucu üzerinde de çalışabilmelidir.

3.3. Yönetim/Log/Raporlama çözümü en az 2 adet aynı marka güvenlik sistemini yönetebilmeli, loglarını saklayabilmeli ve raporlama yapabilmelidir. Kuruma ait aynı marka tüm güvenlik sistemleri yine üreticiye ait aynı arayüz üzerinden yönetilebilmelidir.

3.4. Teklif edilen ürün 11GByte/day log alıp işleyebilme kapasitesine sahip olması tercih sebebidir.

3.4.1. Çözüm güvenlik loglarını filitrelenebilir olarak top sources, applications, destinations, country, policy, web sites, threats, cloud applications,SSL and IPsec VPN olarak gösterebilmelidir.

3.4.2. Çözüm en az **24 TB** disk kapasitesine sahip olmalıdır.

3.4.3. Çözüm anlık olarak filitrelenen yukarıdaki alanlardan çıkan sonuçları anlık olarak gösterebilmelidir.

3.4.4. Çözüm yukarıda sıralanan alanların trafik kullanımını gönderilen/alınan veri boyutları olarak sıralayabilmelidir.

3.4.5. Çözüm kullanıcı entegrasyonu olması durumunda kullanıcı adı yok ise kaynak ip adresi olarak kullanılan uygulama, gidilen web sayfası bilgilerini bant genişliği ayrıntısı ile gösterebilmelidir.

3.4.6. Çözüm log toplanan cihaza ilişkin system event log, admin activity, logging rates gibi bilgileri gösterebilmelidir.

3.4.7. Çözüm son kullanıcılarda yüklü endpoint sistemi loglarını da alarak gösterebilmelidir.

3.4.8. Çözüm anlık olarak tüm trafik log kayıtlarını filitrelenebilir şekilde gösterebilmelidir. Log ayrıntılarında raw format da dahil olmak üzere tüm trafik ayrıntıları yer almalıdır.

3.4.9. Çözüm dahilinde yazılan filitreleri custom log filitresi olarak daha sonra da kullanılmak üzere kaydedebilmelidir.

3.4.10. Çözüm oluşan trafik, sistem ve güvenlik (AV, Application Control, DLP, IPS WebFilter) Event'lerini ele alma mekanizmasına sahip olmalıdır. Ön tanımlı veya özel yazılan event ele alma filitreleri ile belirli event'ler önyüzde görüntülenebilmelidir.

3.4.11. Oluşan Event'ler belirli bir süre aralığında belirli bir adet oluştuğunda mail, snmp trap, syslog olarak harici log altyapısına gönderilebilmelidir.

3.4.12. Teklif edilen ürün saniyede 10000 log alıp işleyebilme kapasitesine sahip olmalıdır.
3.4.13. Teklif edilen ürün 20 cihazdan gelecek logları alabilip herbiri için ayrı yönetsel sanal önyüz sunabilmelidir.
3.4.14. Teklif edilen ürün tercihen bir adet donanımsal, sanal veya cloud sistem olarak önerilebilir.
3.4.15. Teklif edilen ürün eğer sanal ortam için ise vmware ve hyperV desteği olmalıdır.

3.5. Güvenlik sistemlerinden sağlanan loglar üzerinde analiz ve korelasyon yetenekleri bulunmalı bu sayede sistem yöneticilerinin sistemleri gerçek zamanlı ve geçmişe yönelik monitor edebilmeleri ve alarmlar üretebilmesi sağlanabilmelidir.

3.6. Sistem, oluşan olay ve uyarı durumları için e-mail, SNMP trap veya User-Defined script'ler ile alarmlar gönderebilmelidir.

3.7. Yönetim sistemi üzerinde hazır ve özelleştirilebilir dashboard ekranları olmalıdır. Kullanıcıların anlık trafik kullanımları, kurum ağındaki tehlike durumları, kullanıcıların uygulama kullanımları gibi birçok özet bilgi bu dashboard'lar sayesinde görülebilmelidir.

3.8. Sistem üzerinde hazır raporlar bulunmalı, bu raporlar kurum isteğine göre özelleştirilebilmelidir. Bu raporlar istenmesi durumunda CSV veya PDF olarak export edilebilmelidir.

3.9. Loglar üçüncü parti Log sunucularına (SIEM) CSV, veya PDF veya CEF veya SYSLOG veya LEEF formatında gönderilebilmelidir.

3.10. Oluşan olay tiplerine göre SNMP trap yaratmaya imkan tanımalıdır. SNMPv1, SNMPv2c ve SNMPv3 desteklenmelidir.

3.11. Firewall erişim kuralları MS-AD user ve gruplarına kullanmaya imkan tanımalı, bunlar source, destination yönünde kullanılabilmelidir.

3.12. Firewall erişim kuralları uygulamalar temelinde yazılabilmelidir.

3.13. Kurallar üzerinde roll-back imkanı sağlanmalıdır.

3.14. Kurallarda kimin ne sayıda değişiklik yaptığı, kural değiştirdiği veya kural yarattığı izlenebilmelidir.

3.15. Yönetim sistemi tüm kümeleme tekniklerini yönetebilmeli ve en az aşağıdaki bilgileri gösterebilmelidir:

- Aktif ve pasif firewalların durumu
- Gerçek zamanlı olarak güvenlik duvarlarının yük durumu
- Gerçek zamanlı olarak güvenlik duvarları üzerindeki arabirimlerin trafik durumları
- Gerçek zamanlı olarak kesilen veya izin verilen bağlantılar

3.16. Farklı profillerde farklı seviyelerde admin kullanıcı yaratmaya imkan tanımalıdır. Güvenlik kuralları ve gruplarına özel admin hakları atanabilmelidir.

3.17. Read ve write yetkilerinde sınırsız sayıda admin kullanıcılarının yönetim sistemine eş zamanlı olarak bağlanmasına imkan tanımalıdır.

3.18. Admin kullanıcılar en az aşağıdaki sorumluluklara sahip olmalıdır:

- Log takibi
- Screens administration
- Kurallar üzerinde change, create, delete
- Farklı VPN tanımları için set, view, manage

3.19. İzleme ekranlarında, admin kullanıcıların spesifik bir bağlantının ve paketlerin detaylarının izlenmesi mümkün olmalıdır.

3.20. Ekran günlüğünde her bir bağlantı için harcanan süre ve gönderilen/alınan byte miktarları takip edilebilmelidir.

3.21. Konsol üzerinden veya merkezi yönetim platformu üzerinde packet capture alınabilmelidir.

3.22. Yönetim arayüzü ile olan tüm bağlantılar kriptolu yapıda olmalıdır.

3.23. Yönetim arayüzü üzerinden güvenlik sistemlerine ait konfigurasyonlar kolaylıkla backup alınabilmeli ve gerektiğinde restore edilebilmelidir.

3.24. Yazılım güncelleme sırasında olası problemlerde, bir önceki sağlıklı imaja kolayca dönülebilmelidir.

3.25. Yönetim/Log/Raporlama Sisteminin 5 yıl süre ile yazılım güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir ve servis ve güncellemeleri bu süre boyunca sağlanmalıdır.

3.26. Tercih edilen ürünlerin, yapay zeka (AI) entegrasyonu özelliklerine sahip olması, karar verme süreçlerini hızlandırmak ve sistem performansını artırmak amacıyla önem arz etmektedir. AI entegrasyonu sayesinde, ağ güvenliği, trafik analizi ve tehdit tespiti gibi kritik alanlarda otomatikleştirilmiş süreçler ve akıllı analizler sağlanarak, yönetim ve operasyonel verimlilik arttırılması tercih sebebidir.

4. GARANTİ, BAKIM,ONARIM VE DESTEK HİZMETLERİ

4.1. İhale kapsamında teklif edilen ürün ve ürünlerin, **end of sale** (satış sonu) ve **end of support** (destek sonu) tarihleri geçmiş olmamalıdır. Teklif edilen tüm ürünler, üretici tarafından aktif olarak satışta olan ve teknik destek hizmetleri devam eden modeller olmalıdır. Satış ve destek süresi dolmuş ürünlerin kabulü olmayacaktır.

4.2. Sağlanan ürünler için, bakım desteği hizmeti temin edilecektir. Bu destek, sistemin sürekliliğini ve verimliliğini sağlamak amacıyla, gerektiğinde yazılım güncellemeleri, teknik destek ve arıza onarımları gibi hizmetleri içerecektir. Bakım desteği süresince, yetkili teknik personel tarafından sağlanacak destek hizmetleri, belirlenen yanıt süreleri çerçevesinde sunulacak ve sistemin performansının en üst seviyede tutulması için gerekli önlemler alınacaktır.

4.3. Güvenlik duvarı 5 yıl garantili olmalıdır ve garanti üretici tarafından sağlanmalıdır. Garanti kapsamı Priority ve proaktif 7 gün 24 saat 4 saat müdahale esasına göre donanım ve yazılım garanti paketiyle tekliflendirilecektir.

- Garantinin üretici firmadan verildiğine dair belge teklif dosyasında bulunmalıdır.
- Garanti süresi boyunca güvenlik duvarı ile birlikte gelen tüm lisansların güncellemeleri için ek ücret talep edilmeyecektir.
- Garanti süresi boyunca Yüklenicinin İdari veya Teknik şartnamedeki herhangi bir maddeyi yerine getirmemesi durumunda kati teminat mektubu gelir olarak kaydedilebilir.
- Yüklenici firma, ihale kapsamında kurduğu veya teslim ettiği tüm cihaz ve malzemenin envanter birim fiyatı, markası, modeli, modülü ve seri numaralarını liste halinde kuruma teslim edecektir.

5 . EĞİTİM

5.1 Yüklenici eğitim programını İTO'ya sunacaktır.

- Eğitim en az 3 gün sürecektir.
- Eğitim, kurulumlar tamamlandıktan sonra en geç 1 ay içinde verilecektir.
- Eğitim yetkili eğitim kurumu tarafından verilecektir.
- Eğitim sonunda katılımcılara sertifika verilecektir.
- Eğitim 4 Bilgi İşlem Şubesi personeline verilecektir.
- Eğitim programının içeriği kullanılacak uygulamanın ayarlarını yapabilecek ve çıkacak sorunların çözümünü sağlayabilecek seviyede olmalıdır
- Eğitim dili Türkçe olacaktır. Eğitimle birlikte Türkçe eğitim dokümanı verilecektir.
- Eğitim tarihleri ITO yetkilileri tarafından değiştirebilir.

6. TESLİMAT, MONTAJ VE KURULUM HİZMETLERİ

Tüm ürünlerin İTO'ya teslim süresi 45 günü geçmeyecektir.

- Yüklenici , teklifinde sunduğu ürünlerin teslimatını Bilgi İşlem Koordinatörlüğü'nün hazırladığı plan doğrultusunda aşağıdaki lokasyona yapacaktır.
  Eminönü / FATİH : İTO Merkez Bina
- Ürünlerin şartnameye uygunluğu ve eksiksiz olduğu Bilgi İşlem Koordinatörlüğü personeli tarafından tespit edilerek tutanak düzenlenir.
- Yüklenici ilgili ürünü satmaya dair yetkili belgesini ihale dosyasına koyacaktır.
- Yüklenici firma teklifinde sunduğu tüm ürünleri eksiksiz kurmak, gerekli tüm ayar ve entegrasyonları yapmakla ve sistem testleri yapılmış olup sorunsuz şekilde çalışır vaziyette teslim etmekle mükelleftir.
- Yüklenici, ihale kapsamında teslim edilen tüm ürünlerin kurulum ve konfigürasyon işlemlerini yetkilendirilmiş teknik personeller tarafından Bilgi İşlem Müdürlüğü'nün gözetiminde ve kurulum planına göre yapacaktır.
- İTO kaynaklı gecikmeler karşılıklı tutanağa bağlanarak kurulum süresine eklenecektir.