15.01.2014

ÜNİTESİ : Satın Alma Müdürlüğü
SAYI : 2014/1164
KONU : **TÜRKİYE FUTBOL FEDERASYONU**
AĞ GÜVENLİK DUVARI SİSTEMİ VE LOGLAMA İŞİ

SON BAŞVURU TARİHİ : 27 Ocak 2014 Saat 15.00

Türkiye Futbol Federasyonu'nda kullanılmak üzere aşağıda teknik detayları verilen Ağ Güvenlik Duvarı Sistemi ve Loglama işi alımı yapılacaktır. İstekliler, tekliflerini kapalı zarf usulü veya posta yoluyla İstinye Mah Daruşşafaka Cad. No 45 Kat.2 adresinde mukim Türkiye Futbol Federasyonu Satın Alma Müdürlüğüne 27 Ocak 2014 Saat 15.00 e kadar teslim edebilirler.

ahmeteksi@tff.org mail adresinden veya 0 212 362 22 98 no'lu telefondan detaylı bilgi alınabilir.

Teklif Sahibi aşağıda belirtilen belgeleri dosyasında teslim edecektir:

a. Tebligat için adres beyanı, telefon numarası, faks numarası ile elektronik posta adresi,
b. Mevzuat gereği kayıtlı olduğu ticaret ve/veya sanayi odası belgesi,
c. Teklif vermeye yetkili olduğunu gösteren noter tasdikli imza beyannamesi veya imza sirküleri,
d. Referans dosyası,
TFF 4734 sayılı Kamu İhale Kanununa tabii olmayıp, teklifleri değerlendirip değerlendirmemekte, dilediği istekliye işi vermekte serbesttir.
TFF, söz konusu teklifleri e-ihale sistemine dahil etme hakkını saklı tutar

Ağ Güvenlik Duvarı Sistemi ve Loglama Teknik Şartnamesi

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.

1.2. Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlanmalıdır. 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.

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

1.4. Teklif edilen Ağ Güvenlik Duvarı, yedekli çalıştırılacak şekilde 2 adet teklif edilecektir. İki cihaz High-Availability özelliğinde çalışmalıdır. 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.

1.5. 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. Cluster ünitelerinin her ikisi de SNMP ile gözlemlenmek istendiğinde opsiyonel olarak dedike yönetim portu ayarlanabilmeli ve yönetimsel erişimler için ayrı bir default gateway verilebilmelidir.

1.6. Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır. Gerektiğinde bu denetim geçici olarak devre dışı bırakılabilmelidir

1.7. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır. Bu kontrol ve denetim otomatik olarak routing tablosu üzerinden gerçekleştirilmelidir. Ayrıca bir tanım yapmaya gerek kalmamalıdır. Troubleshooting için gerektiğinde spoofing denetimi geçici olarak devre dışı bırakılabilmelidir.

1.8. 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 bir fiziksel arayüz altında en az 1000 adet VLAN tanımlanmasına izin vermelidir.

1.9. Sistem Sanal Güvenlik Duvarı özelliği ile teklif edildiği durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları güvenlik kuralları, fonksiyonları ve yönlendirme tabloları açısından birbirinden bağımsız olarak çalışabilmelidir.

1.10. 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.

1.11. Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;

1.11.1. SPI (stateful packet inspection),
1.11.2. Saldırı Tespit ve Engelleme Sistemi (IPS)
1.11.3. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
1.11.4. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü

1.11.5. URL Kategori Filtreleme

1.12. Routing modda aşağıdaki özellikleri sağlamalıdır;
- 1.12.1. SPI (stateful packet inspection),
- 1.12.2. IPSec VPN Sonlandırma,
- 1.12.3. SSL VPN Sonlandırma,
- 1.12.4. Saldırı Tespit ve Engelleme Sistemi (IPS)
- 1.12.5. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
- 1.12.6. Virüs/Zararlı İçerik Kontrolü
- 1.12.7. URL Kategori Filtreleme
- 1.12.8. Bant genişliği kontrolü
- 1.12.9. Statik yönlendirme (static routing),
- 1.12.10. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
- 1.12.11. Sunucu yük dengeleme
- 1.12.12. WIFI Access Point kontrolcüsü

1.13. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, 10 adede kadar farklı Internet bağlantısını yedekli/yük dağıtımlı olarak kullanabilmelidir.

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

1.15. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.

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

1.17. Güvenlik duvarı politikaları ve desteklenen diğer güvenlik fonksiyonları kullanıcı ve/veya kullanıcı grupları bazında uygulanabilmelidir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır. NTLM yetkilendirmeyi desteklemeli ve bu sayede sisteme logon bilgisi bir şekilde gelmemiş bir kullanıcıyı dahi AD grup haklarına göre otomatik yetkilendirebilmelidir.

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

- 1.18.1. Kaynak, hedef, ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
- 1.18.2. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
- 1.18.3. İstenildiğinde per-IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural üzerinden izin verilen her kaynak için tanımlanan bant genişliğinin garanti edilmesi sağlanmalıdır.

1.18.4. Madde-1.17.3 un aksine tüm aynı kural dahilinde izin verilen her kaynak için tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.

1.18.5. Uygulama bazında bant genişliği kontrolü yapabilmelidir.

1.18.6. Aynı trafik ile ilgili Inbound ve outbound doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.

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

1.20. Politika bazlı firewall'un oturumlarda start/stop loglayıp / loglamaması denetlenebilmelidir.

1.21. Firewall, NAT ve sunulan tüm layer7 güvenlik fonksiyonları granüler şekilde "sadece belirlenen kriterlere uyan trafik için" kural bazlı devreye alınabilmelidir.

1.22. WebGUI üzerinden günlük operasyon işlemleri büyük oranda (CLI üzerinde işlem yapmaya gerek olmadan) gerçekleştirilebilmelidir. CLI üzerinden ise tüm konfigürasyona bulk şekilde müdahale edilebilmelidir.

1.23. 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 (üç bin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulamalar davranışlarına, teknolojilerine, risk seviyelerine, işlevlerine vb.. göre otomatik kategorize edilmiş olmalı ve kolayca istenen denetimler devreye alınabilmelidir. Web 2.0 özellikleri ile örneğin facebook read only erişimine izin verilip, facebook içerisindeki her türlü chat, video, uygulama, oyun vb.. engellenebilmelidir. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.

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

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

1.26. 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.

1.27. İhtiyaca göre kişisel IPS ve Uygulama Kontrolü imzaları yazılmasını desteklemelidir.

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

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

1.30. Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.

1.31. Kullanıcı trafiklerinin davranış analizini yaparak, anormal davranış gösteren kullanıcı makinalarının grafiksel arayüzde kolayca tesbitine olanak sağlamalıdır. Firewall üzerinden bloklanan trafikler, uygunsuz web kategorilerine erişim denemeleri, riskli uygulamaların çalışıyor olması, botnet siteleri ile haberleşme gibi layer3-layer7 arası tüm davranışlar ağırlığı belirlenebilir puanlama ile belirlenebilmelidir. Bu sayede henüz imzası yayınlanmamış bir sıfır-gün aktivitesinin tesbit edilmesi amaçlanmaktadır.

1.32. 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.

1.33. SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.

1.34. SSL VPN özelliği sınırsız kullanıcı lisansı ile teklif edilecektir.

1.35. 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.

1.36. SSL VPN ve IPSEC 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, QoS ve Bant Genişliği yönetimi özellikleri uygulanabilir olmalıdır.

1.37. Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP, POP3, IM (ICQ, MSN, Yahoo Messenger) , MAPI, HTTPS, SMTPS, POP3S, IMAPS, FTPS, SMB 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

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

1.39. 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.

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

1.41. Sistemde en az 75 adet URL kategorisi ve 250 milyondan fazla kategorize edilmiş URL bulunmalıdır.

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

1.43. URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin *.org.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.

1.44. URL filtreleme uyarı ekranları özelleştirilebilecektir.

1.45. 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. IPv6 trafiğine IPS, Uygulama Denetimi ve Web Filtreleme yapılabilmelidir.

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

1.47. Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir

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

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

1.50. Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 1 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 1 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

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

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

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

1.52.6. Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http adresinin kontrolü ile ve ping ile kontrol edebilmelidir.

1.53. Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.

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

1.55. Web cache özelliği olmalıdır.

1.56. Web cache communication Protocol (WCCP) desteği olmalıdır.

1.57. Sistem eş zamanlı 7 Milyon oturumu desteklemeli ve saniyede en az 190.000 yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün dokümanlarında belirtilmiş olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.58. Güvenlik Duvarı Sisteminin 512 byte UDP paketleri için en az 8 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.

1.59. Sistem Site-to-Site ve Client-to-Site için en az 10.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir.

1.60. Firewall işlevi gerçekleştirirken, hassas trafikler için sadece 6 microsaniye gecikme (latency) yaratması tercih nedenidir.

1.61. Firewall 64 byte UDP paketleriyle 30 milyon pps desteklemelidir.

1.62. Sistem 6 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.

1.63. Sistem üzerinde En az 12 adet 10/100/1000 Base-T, 8 adet GbE SFP, 2 adet 10 GbE SFP+ bağlantı noktası olmalıdır.

1.64. Güvenlik Sistemi üzerinde en az 128 Gbyte kapasitede HDD Depolama alanı bulunmalıdır. Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama Sistemine kayıt gönderebilmeli ve sistem üzerindeki Depolama Biriminde de kayıt Tutabilmelidir.

Güvenli Duvarı Loglama ve Raporlama Sistemi

1) Önerilen güvenlik duvarı sistemini kayıt depolama ve takibini, raporlama işlemlerini gerçekleştirmek için aşağıda belirtilen şartlara uyan kayıt takip ve raporlama ürün/ürünleri alınacaktır.
2) Log kayıt alanı olarak en az 1TB depolama alanını destekleyecektir.
3) Bu çözümün Vmware ESX (Vmware vSphere) üzerinde çalışacak şekilde teklif edilmelidir.
4) Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.
5) Olay tanımlarına öncelik derecesi atanabilecektir.
6) Cihaz üzerinden geçen tüm trafiğin günlüklerde tutulması, istenen kıstaslara göre (En az IP, IP aralığı, ağ, protokol, zaman) filtrelenebilmesi ve aktif bağlantıların gerçek zamanlı izlenebilmesi sağlanacaktır.
7) Alınan ve gönderilen paket büyüklüklerini gösterebilecektir.
8) Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.
9) Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilecektir.
10) Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.
11) Merkezi yönetim dâhilinde bulunan bileşenlere ait anlık ortalama CPU, boş disk alanı, firewall, firewall cluster üzerinden akan tüm uygulamalar, kullanıcı IP adresleri ve dâhili kullanıcı isimleri gibi değerler anlık ve sürekli olarak görüntülenebilecektir.
12) 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.

13) Tutulan kayıt alanları baz alınarak özelleştirilmiş sorgular yazılabilmeli ve bu sorguların çıktıları, tablo, pie-chart şeklinde raporlar içerisine konulabilecektir.

14) PDF formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle belirlenen zamanlarda gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilecektir.

15) Teklif edilen sistemlerin en az 2 yıl donanım garantisi bulunmalıdır. 2 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.