Ağ Güvenlik Duvarı Sistemi – 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 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.

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. Yedeklilik konfügrasyonunda her segment için güvenlik duvarı üzerinde set edilecek Ip sayısı 1 (bir) adet olabilmelidir. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.

1.5. Sistem üzerinde en az 2 Adet 10Gbit/s SFP+ interface, 8 adet SFP, 10 Adet RJ45 1Gbit/s interface olmalıdır.

1.6. Cihaz üzerinde yedek güç kaynağı takılı olarak teklif edilmelidir.

1.7. Sistem herbir cihaz için 2 adet 10Gbit SFP+ connector ile teklif edilmelidir.

1.8. Sistem loglama amaçlı 480GByte SSD disk desteğine sahip olmalıdır.

1.9. Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.

1.10. Sistem bulut sandbox özelliği sayesinde sıfırıncı gün atakların analizini yapabilmelidir.

1.11. Bulut sandbox özelliği firewall ile entegre şekilde sınırsız dosya gönderimi desteğine sahip olmalıdır.

1.12. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır, anti-spoof özelliğine sahip olmalıdır.

1.13. 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.

1.14. 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.

1.15. 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.

1.16. Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
- 1.16.1. SPI (stateful packet inspection),
- 1.16.2. Saldırı Tespit ve Engelleme Sistemi (IPS)
- 1.16.3. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
- 1.16.4. Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
- 1.16.5. URL Kategori Filtreleme

1.17. Routing modda aşağıdaki özellikleri sağlamalıdır;
- 1.17.1. SPI (stateful packet inspection),
- 1.17.2. IPSec VPN Sonlandırma,
- 1.17.3. SSL VPN Sonlandırma,
- 1.17.4. Saldırı Tespit ve Engelleme Sistemi (IPS)
- 1.17.5. Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
- 1.17.6. Virüs/Zararlı İçerik Kontrolü
- 1.17.7. URL Kategori Filtreleme
- 1.17.8. Bant genişliği kontrolü
- 1.17.9. Statik yönlendirme (static routing),
- 1.17.10. RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
- 1.17.11. Sunucu yük dengeleme

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

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

1.20. Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.

1.21. Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü (interface) ve/veya zone bazlı yazılabilmelidir.

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

1.23. Kullanıcı bazında NAT kuralı yazılabilmelidir.

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

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

1.24.3. 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.

1.24.4. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.

1.24.5. Uygulama bazında bant genişliği kontrolü yapabilmelidir.

1.24.6. 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.

1.25. Ağ Güvenlik Duvarı Sistemi kendi üzerinde tanımlanan kullanıcı veritabanı, harici RADIUS ve LDAP sunucuları üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir. SSLVPN, client-site IPSEC VPN, internet erişimi gibi senaryolar için bu özellik kural bazlı devreye alınabilmeli ve kullanıcı takibi (kullanıcı ismi, grubu, yarattığı trafik, kalan süre vb..) gibi detaylar GUI üzerinden gözlemlenebilmelidir.

1.26. Aktif dizin entegrasyonu ağ güvenlik duvarı üzerinden sorgu çekme yöntemiyle veya domain üyesi herhangi bir sunucu üzerine kurulacak ajan yardımıyla gerçekleşebilmelidir. Sistemin temel çalışmasında son kullanıcı makinalarına bir yazılım kurulması ihtiyacı bulunmamalıdır.

1.27. Domain entegrasyonu sonucunda bir nedenden (Windows ortamı vb..) firewall ile senkronize edilememiş kullanıcıların firewall üzerinden geçerken anında tanınabilmesi için NTLMv2 gibi güvenli alternatif yöntemler kullanılabilmelidir.

1.28. Ağ Güvenlik Duvarı Sistemi aktif dizin ile entegre edildiğinde ip/subnet/vlan/zone bazlı tanımlamalara ek olarak kullanıcı ve grup bazlı güvenlik politikaları yazılmasını desteklemelidir. Kullanıcı ve grup tanımlamaları politika ekranından arkadaki aktif dizin üzerinden otomatik filtrelenerek getirilen user, security group veya OU tanımları içerisinden çoklu-seçim ile tek adımda gerçekleştirilebilmelidir. Bu sayede farklı kullanıcı profillerine farklı güvenlik politikaları uygulanabilmelidir.

1.29. Ağ Güvenlik Duvarı Sistemi üzerinde güvenlik politikaları ip/subnet, interface (fiziksel/VLAN), zone, kullanıcı, grup (OU veya Security Group) haricinde cihaz tipi bazlı da yazılabilmelidir. Windows, Linux, Android, Iphone vb.. gibi hazır tanımlı cihaz kategoriler haricinde kişiselliştirilmiş cihaz tanımlamaları (el terminalleri, printer vb..) yapılabilmelidir.

1.30. 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.

1.31. Ağ Güvenlik Duvarı Sistemi Web 2.0 uygulamaları içerisindeki alt uygulamaları (facebook.chat, facebook.games vb.. gibi) ayırt edebilmeli ve sosyal medya uygulamalarına read-only erişimi (facebook açılsın ama oyun oynanamasın, chat fonksiyonu kullanılamasin vb.. gibi) mümkün kılabilmelidir.

1.32. Ağ Güvenlik Duvarı Sistemi uygulama veya kategori bazlı blok, reset, allow, log, karantina aksiyonlarını alabilmelidir.

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

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

1.35. 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.

1.36. IPS sistemi en az 7000 (yedibin) imzaya sahip olmalıdır.

1.37. 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.

1.38. Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını ve aynı zamanda atak yapılan sistemlere olan erişimi belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapılan sistem olası ataklara karşı koruma altına alınabilmelidir

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

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

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

1.42. 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.

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

1.44. SSL VPN özelliği en az 300 kullanıcı lisansı ile teklif edilecektir.

1.45. 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.

1.46. 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.

1.47. 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

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

1.49. 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.

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

1.51. Sistem üzerinde en az 70 adet URL kategorisi bulunmalıdır, en az 250milyon URL sınıflandırılmış olmalıdır.

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

1.53. 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.

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

1.55. 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.

1.56. URL/Application kontrol/Anivirus filtreleme uyarı ekranları özelleştirilebilecektir.

1.57. 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.

1.58. Sistem IPv6 için DDoS profiline sahip olmalıdır.

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

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

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

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

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

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

1.65. Sistem, içeri doğru NAT Load-Balance özelliği ile internetten gelen istekleri birden fazla sunucuya yönlendirebilmelidir. Örneğin, iç ağda bulunan ve aynı servisi veren iki web server veya terminal server arasında trafik paylaşımı bu özellik sayesinde yapılabilmelidir. Eğer web server veya terminal server'lardan birisi devre dışı kalırsa diğer web server veya terminal server herhangi bir müdahaleye gerek kalmadan hizmetine devam edebilmelidir.

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

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

1.66. Explicit proxy özelliği desteklenmelidir.
1.67. Sistem TCP eşik değeri temelli DoS/DDoS koruması saglayabilmelidir.
1.68. 10 adet sanal güvenlik duvarı desteği standart lisans ile verilebilmelidir.
1.69. Sistem WAN tarafında optimizasyon ve yük dağılımı desteği olmalıdır.
1.70. Sistem wan link load balance özelliğine sahip olmalıdır ve internet çıkışı oransal olarak ilgili dış hatlara yönlendirilebilmelidir.
1.71. Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.
1.72. Web cache özelliği olmalıdır.
1.73. Sistem WAF (Web Application Firewall) profillerini desteklemelidir. Bu oluşturulan profiller kural temelli olarak tanımlanabilmelidir.
1.74. Web cache communication Protocol (WCCP/ICAP) desteği olmalıdır.
1.75. Sistem WAF (Web Application Firewall) profillerini desteklemelidir. Bu oluşturulan profiller kural temelli olarak tanımlanabilmelidir.
1.76. Sistem VOIP güvenlik profillerine sahip olmalıdır ve kural temelli olarak uygulanabilmelidir.

a. Güvenlik Duvarı Performans Değerleri

1.1. Teklif edilen Ağ Güvenlik Duvarı, yedekli aktif-aktif/aktif-pasif olarak çalışabilme özelliğine sahip olmalıdır ancak 1 adet teklif edilecektir

1.2. Teklif edilen güvenlik sistemi, teklif edilen konfügürasyonda, 1518/512/64 Byte IP paket büyüklüklerinin hepsi için en az 27 Gbit/sec 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.

1.3. Sistem aynı anda en az 8 milyon oturumu desteklemeli ve saniyede en az 450 bin 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.

1.4. Güvenlik Duvarı Sistemi en az 15 Gbit 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.

1.5. Güvenlik Duvarı Sistemi en az 8 Gbps SSL inspection throughput değerine sahip olmalıdır. Bu performans degieri IPS açık iken HTTP trafiğinin TLS v1.2 with AES256-SHA 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.

1.6. Sistem Site-to-Site için en az 1000 adet, Client to site için 2000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir

1.7. Sistem 10 Gbit/s Enterprise MIX 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.

1.8. Sistem 7 Gbit/s Thread Prevention (Malware kontrol, Application kontrol, IPS) throughput performans değerine Enterprise trafic MIX veya gerçek trafik değeri olarak sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.9. Sistemin; Firewall, VPN, 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 sistemle birlikte verilmelidir.

1.10. Teklif veren firma teklif ettiği ürünlerin yetkili satıcısı olduğuna dair ürünün Türkiye distribütöründen yetkili satıcı belgesini teklifinde sunmalıdır

1.11. Teklif veren firma kurumun mevcut fortigate 1200d cihazı üzerindeki ayarları kurumun istediği şekilde teklif verdiği ürüne aktaracak ve devreye alacaktır.

1.12. Teklif veren firma teklif verdiği ürün için ürün lisans süresi boyunca uzaktan teknik destek verecektir. Uzaktan çözülemeyen ve kurumun hizmet vermesini aksatan teknik sorunlarda herhangi bir ücret talep etmeksizin yerinde destek verecektir.

1.13. Teklif veren firma teklif ettiği ürünle ilgili kurumun belirlediği 1(bir) kişiye kurumda 2 (iki) gün eğitim verecektir. Eğitim ileri düzey olacaktır.