DOĞUŞ ÜNİVERSİTESİ

AĞ GÜVENLİK SİSTEMLERİ

TEKNİK ŞARTNAMESİ

İÇİNDEKİLER

1. AMAÇ

1.1. Doğuş Üniversitesinin belirttiği lokasyonda devreye alınacak olan 2 adet güvenlik duvarı cihazı (UTM) cihaz , loglama-raporlama ,mail ve kimlik yönetimi yazılımı lisans ve kurulum destek hizmetleri alımını kapsamaktadır.

1.2. Kurulumlar kurumun belirttiği şekilde yapılacaktır. Mevcut sistemde yeni sistemlere geçişi ile alakalı teknik destek yüklenici tarafından verilecektir.

1.3. Kurumun bilgi işlem personeli talebi üzerine gerekli olan konfigürasyonlar kurulum esnasında yapılacak ve bu iş için ekstra ücret alınmayacaktır.

1.4. Kurulum hali hazırdaki sistem ile eş zamanlı devreye alınacaktır, bununla birlikte geçiş aşamasında sistemin çalışabilmesi için kullanılabilecek geçici donanım ve yazılım gereksiniminde firma ilave bir ücret talep etmeyecektir.

2. KAPSAM:

YENİ NESİL FİREWALL UTM-

Ağ Güvenlik Duvarı Sistemi

Ağ Güvenlik Duvarı Ürünü aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini desteklemeli ve sağlamalıdır.

Kurum bünyesinde çalışan aşağıdaki teknik özelliklere sahip yedekli yapıda çalışacak (aktif-pasif) 2 adet güvenlik duvarı ürünü için yine aşağıdaki maddeleri kapsayan ilgili lisanslar 3 yıl süre ile teklif edilmelidir.

Ağ Güvenlik Duvarı Sistemi

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, her hâlükârda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.

1.4. Teklif edilen Ağ Güvenlik Duvarı 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.

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

1.7. Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır

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.

1.9. 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.

1.10. 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
- 1.12.13. WAN optimizasyon
- 1.12.14. Web Cache

1.13. Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda 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, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.

1.18. Kullanıcı bazında NAT kuralı yazılabilmelidir.

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

1.19.1. Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
1.19.2. Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
1.19.3. 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.
1.19.4. Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
1.19.5. Uygulama bazında bant genişliği kontrolü yapabilmelidir.
1.19.6. 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.

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

1.21. 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.

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

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

1.24. 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.

1.25. 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.

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

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

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

1.29. 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.

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

1.31. SSL VPN özelliği en az 10.000 kullanıcı lisansı ile teklif edilecektir.

1.32. 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.

1.33. 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.

1.34. 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

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

1.36. 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.

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

1.38. Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.

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

1.40. Çözüm sıfır-gün ataklarına karşı, bulut tehdit engelleme sistemleri ile entegre olmalı, bu sayede koruma seviyesini arttırmalı ve potansiyel hatalı tespit sayılarını azaltabilmelidir. Sıfır-gün ataklarına karşı koruma sağlamak için, Firewall'lar üzerine eklenebilecek bulut tehdit engelleme sistemleri lisansları 3 yıl geçerli olacak şekilde teklif edilmelidir.

1.41. 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.

1.42. İstenildiğinde categorilerden bağımsız olarak, sisteme eklenebilecek tam URL bilgisi (Örneğin: www.abc.com/deneme/sayfa1.php) bazında engelleme yapabilmelidir.

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

1.44. 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.

1.45. URL filtreleme uyarı ekranları özelleştirilebilecektir.

1.46. 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.

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

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

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

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

1.51. Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel "Network Firewalls" için "Gartner Magic Quadrant" tablosunda yer almalıdır.

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

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

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

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

1.54. Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.

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

1.56. Wan optimizasyon özelliklerine sahip olacaktır.

1.57. Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.

a. Güvenlik Duvarı Performans Değerleri

Teklif edilen Ağ Güvenlik Duvarı 2 adet yedekli olarak teklif edilecektir.

1.58. Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda en az 130 Gbps Firewall 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.

1.59. Her bir Ağ Güvenlik Duvarı ünitesi Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az 10,5 Gbps kapasiteye sahip olmalıdır. Bu kapasite kullanıcı/istemci arasındaki istek-cevap trafiğinin toplamına (çift yönlü analiz ile) bu güvenlik özelliklerinin uygulandığı konfigürasyonda belirlenmiş olmalıdır. Belirtilen bu değer ürün kataloglarında yer almalıdır. Ürün kataloglarında Tehdit Koruma için farklı terminoloji kullanılmış ise bu koşulda ürün kataloğunda NGFW (Firewall + IPS + Uygulama Denetimi) kapasitesi gerçek ortam değeri baz alınarak en az 11,5 Gbps olmalıdır.

1.60. Sistem aynı anda en az 8 milyon oturumu desteklemeli ve saniyede en az 550.000 yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.61. Güvenlik Duvarı Sistemi en az 50 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.

1.62. Sistem Site-to-Site için en az 2.000 adet, Client to site için 50.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir.

1.63. Sistem 14 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.

1.64. Sistem üzerinde;
- 1.64.1. En az 4 adet 25GE SFP28/10GE SFP+ ara yüz bulunmalıdır.
- 1.64.2. En az 4 adet 10GE SFP+ ara yüz bulunmalıdır.
- 1.64.3. En az 8 adet 1GE SFP ara yüz bulunmalıdır.
- 1.64.4. En az 16 adet 1GE RJ45 ara yüz bulunmalıdır.

1.65. Sistem Syslog Sunuculara ve Kayıt/Raporlama Sistemine kayıt gönderebilmelidir.

1.66. Sistemin; Firewall ve 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

b. *KİMLİK DOĞRULAMA*

Kimlik Doğrulama ürünü aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır

c. Kimlik dogrulama Kapasite

1. Teklif edilen ürün 200 adet anlık local veya uzak kullanıcı desteğine sahip olmalıdır.
2. Teklif edilen ürün 5 adet CA (Certificate autority) desteğine sahip olmalıdır.
3. Teklif edilen ürün 200 adet kullanıcı sertifika desteğine sahip olmalıdır.
4. Teklif edilen ürün 10 adet kullanıcı grubu oluşturma desteğine sahip olmalıdır.
5. Teklif edilecek ürün donanım olarak veya sanal olarak VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0 / 5.5 / 6.0, Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2 ortamlarında çalışabilmelidir.
6. Teklif edilen ürün tek olarak lisanslanmalı ve gerektiğinde yedekli Active-Passive HA ve Config Sync HA desteğine sahip olmalıdır.

d. Kimlik dogrulama özellikleri

1. Teklif edilecek ürün SSO (single sign on) desteği olmalıdır ve aşagıdaki kaynaklardan beslenebilmelidir.

    a. AD (Active directory) sorgulama (AD polling) veya AD agent iletişimi
    b. TS (Terminal server) agent
    c. Kerberos
    d. REST API
    e. Radius Accounting
    f. FortiClient SSO client
    g. SSO Login Portal
    h. Syslog
2. Teklif edilecek ürün Windows altyapılar için WMI sorgulama yöntemi ile aktif olmayan kullanıcıları SSO listesinden çıkartabilmelidir veya belli bir süre limiti ile SSO listesinden çıkartabilmelidir.
3. Teklif edilecek ürün kablosuz altyapılar için merkezi kimlik doğrulama sistemine sahip olmalıdır.
4. Teklif edilecek ürün kablosuz altyapılar için kullanıcılar için PEAP, EAP-TTLS desteği olmalıdır aynı zamanda sertifika tabanlı EAP-TLS BYOD (bring your own device) desteğine sahip olmalıdır.
5. Teklif edilecek ürün kablosuz altyapılar için mobil telefon doğrulamalı konuk yönetimi captive portal çözümüne sahip olmalıdır.
6. Teklif edilecek ürün kablosuz altyapılar için konuk captive portal çözümü admin onayı ile kullanıcı şifrelerini HTTP/HTTPS/mail-to-sms servislerine entegrasyonuna sahip olmalıdır.
7. Teklif edilecek ürün kablosuz altyapılar için konuk captive portal çözümü değiştirilebilir önyüz desteğine sahip olmalıdır.
8. Teklif edilecek ürün kablosuz altyapılar için SSO desteği ile Fortinet firewall'lara direk entegre olabilmelidir.
9. Teklif edilecek ürün kablosuz altyapılar için konuk yönetimi captive portal çözümü facebook, twitter, Google vb. Kimlik bilgileri ile giriş desteğine sahip olmalıdır.
10. Teklif edilecek ürün kablosuz altyapılar için konuk yönetimi belli bir sürede ilgili kullanıcıların resetlenmesini ve sistemden silinmesini desteklemelidir.
11. Teklif edilen ürün sertifika yönetimi yapabilmelidir.
12. Teklif edilecek ürün kullanıcı sertifika yönetimi aşagıdaki bağlantılar için oluşturup doğrulayabilmelidir.
    a. VPN
    b. Kablosuz 802.1X(PEAP,EAP)
    c. Windows desktop authentication
    d. FTK300 USB PKI Certificate Store uyumluluğu
    e. KAblo NAC destegi 802.1X (PEAP, EAP-TTLS, EAP-TLS, EAP-GTC)
13. Teklif edilen ürün Radius Accounting Proxy desteği olmalıdır.
14. Teklif edilen üründe MAC cihaz kimlik doğrulama desteği olmalıdır.
15. Teklif edilen ürün harici AD, LDAP, Radius desteği olmalıdır.
16. Teklif edilen ürün LDAP server olarak kullanılabilmelidir.
17. Teklif edilen ürün Radius ürün olarak kullanılabilmelidir.
18. Teklif edilen ürün Token yönetimi yapabilmelidir. Lisans kadar soft veya hardware token register edilebilmelidir.
19. Teklif edilen ürün üzerinden adil kullanım kotası amaçlı kota temelli bant genişliği yönetimi yapılabilmelidir.

Yönetim özellikleri

1. Teklif edilen ürün HTTPS üzerinden yönetilebilmelidir.
2. Teklif edilen ürün kullanıcı girişlerini kayıt altına alabilmeli ve harici loglama sistemlerine aktarabilmelidir.
3. Teklif edilen ürün CPU ve memory kullanımlarını, kullanıcı adet istatistiklerini önyüz üzerinden gösterebilmelidir.
4. Teklif edilen ürün otomatik backup alarak belirlenen zamanda harici ftp sitesine gönderebilmelidir.
5. Teklif edilen ürün SNMP v1/v2c ve v3 destegi olmalıdır. MIB bilgileri üzerinden soğulama yapılabilmelidir.
6. Teklif edilen ürün admin kullanıcılarına yetkilendirme yapılabilmelidir.

7. Teklif edilen ürün log kayıtları HTTPS arayüz üzerinden filitrelenebilir şekilde sorgulanabilmelidir.
8. Teklif edilen ürün log kayıtlarını harici syslog server'lara gönderebilmelidir.
9. Teklif edilen ürün 3 (üç) yıllık yazılım destek paketi ile verilmelidir.

Email Security VM02 – 3 YIL

1) Teklif edilecek e-posta koruma sistemi, kuruma gelen e-postalar üzerinde Spam, zararlı yazılım ve oltalama (phishing) içeriklerini tespit edecek ve engelleyebilecektir.

2) Sistem sıkılaştırılmış, üreticiye ait işletim sistemi üzerinde çalışmalıdır.

3) Sistem, şartnamede istenen özellikleri tek bir donanımsal (Donanım / Yazılım Bütünü) çözüm veya sanal yazılımsal çözüm olarak sağlamalıdır.

4) IPv6 desteği olmalıdır.

5) Teklif edilen e-posta koruma sistemi, aynı anda E-posta Sunucuya doğru (Inbound) ve E-posta Sunucudan dışarı (Outbound) e-posta trafiğinde güvenlik sağlayabilmelidir.

6) E-postalar üzerinde yapılacak taramalar bellek (memory) üzerinde yapılmalı ve içerik analizi için kuyruk kullanımı gerektirmemelidir.

7) Erişim Kontrol kuralları ile belirlenen gönderici ve alıcı arasındaki e-posta iletişiminin taranması ve/veya taranmadan iletilebilmesi sağlanabilmelidir.

8) Alıcı ve gönderici adres tanımlamaları regex ifadesi kullanarak yazılabilmelidir.

9) IP bazlı politikalar ile kaynak ve hedef IP veya IP grupları arasındaki trafik için uygulanacak smtp protokol ve içerik taraması kontrol edilebilmelidir.

10) Sistem üzerinden IP bazında bağlantı sınırı, her bir bağlantı üzerinden gönderilebilecek e-posta sayısı ve e-postaların maksimum alıcı adres sayısı belirlenebilmelidir.

11) Gönderici doğrulaması için SPF kontrolü olmalıdır.

12) Spam engelleme politikası, e-posta adresi, IP adresi veya domain parametreleri bazında yapılabilmelidir.

13) Teklif edilen E-posta Güvenlik Sistemi, E-posta Sunucuya doğru (Inbound) e-posta trafiğinde:

57.1)DOS saldırılarını engelleme (mail bombing),

57.2)Spam ve Phishing Engelleme,

57.3)Virus, Spyware ve Malware engelleme,

57.4)İhtiyaç durumunda, kanuni gerekçelerle E-posta trafiğinin arşivlenmesi fonksiyonlarını sağlamalıdır.

14) Sistem DOS ataklarına karşı aşağıdaki metotları kullanarak engelleme yapabilmelidir.

58.1)Belirlenen zaman içerisinde her istemci bazında bağlantı sayısı

58.2)Her istemci için eş zamanlı bağlantı sayısı

58.3)Toplam eş zamanlı bağlantı sayısı

58.4)Her oturum bazında gönderilebilecek e-posta sayısı

58.5)E-posta içerisinde bulunabilecek alıcı sayısı

58.6)Alıcı ve gönderen adresleri içeren yasaklı ve izinli e-posta adres listeleri

15) Teklif edilen E-posta Güvenlik Sistemi, E-posta Sunucudan dışarı doğru (Outbound) e-posta trafiğinde:

59.1)E-posta sunucudan dışarıya doğru spam engelleme yaparak, kurumun Spam kara listelerine (RBL, DNSBL) girmesini engelleme,

59.2)Spam ve Phishing Engelleme,

59.3)Virus, Spyware ve Malware engelleme,

59.4)Spam Zombie'lerini ve Bot'larını engelleme,

59.5)İhtiyaç durumunda, kanuni gerekçelerle E-posta trafiğinin arşivlenmesi fonksiyonlarını sağlamalıdır.

16) E-posta Güvenlik sistemi aşağıdaki metodları kullanarak Spam engelleme yapabilmelidir

60.1)IP bazında engelleme,

60.2)İçerik Filtreleme,

60.3)E-posta Domain ve E-posta adres tabanlı Black/White listelerine göre filtreleme,

60.4)E-posta Header inceleme

60.5)RBL ve DNSBL bazlı Filtreleme,

60.6)E-posta içeriğindeki olabilecek URL ler bazında Filtreleme,

60.7)Kullanıcı/Domain bazlı Bayesian filtreleme,

60.8)Dinamik Heuristic kural güncellemeleri ile filtreleme,

60.9)Greylist,

60.10)]İmaj analiz ile filtreleme,

60.11)PDF dosyası içinde içerik tarama,

60.12)Anahtar kelime bazlı içerik filtreleme

60.13)İstenmeyen eklenti türlerini filtreleme

60.14)Bulut istihbarat tabanlı filtreleme.

17) Taranan maillerde zararlı ya da istenmeyen içerik tespit edildiğinde aşağıdaki aksiyonlar alınabilecektir.

61.2)İletme

61.3)Mailin içeriğinde, konusunda, değişiklik yaparak iletme

61.4)Alıcıya ya da belirlenen alıcılara maili ekte iletme

61.5)Alıcıya ya da belirlenen alıcılara uyarı ve bilgilendirme gönderme

61.6)Göndericiye hata mesajı gönderme

61.7)Göndericiye hata göndermeden maili düşürme

61.8)Karantinaya alma

61.9)Mailin konusuna ya da içeriğine istenilen uyarı mesajı ekleme

18) Sistem, aşağıdaki SMTP fonksyonlarını destekleyecektir

62.1)RFC5321 SMTP desteği

62.2)RFC3207 Secure SMTP over TLS desteği

62.3)RFC4871 DKIM signing and verification desteği

62.4)RFC4408 Sender Policy Framework verification desteği

19) E-posta koruma sistemi e-postlara eklenerek gönderilebilecek zararlı yazılımları tespit edebilecek ve engelleyebilecektir. Zararlı yazılım tespit imza veritabanı üretici tarafından internet üzerinden güncellenmelidir.

20) Reverse DNS kontrolü yapabilmelidir.

21) Şifreleme desteği olmalıdır.

22) Herhangi bir politika sebebi ile engellenmesi gereken e-postalar karantinaya alınabilmeli, istendiği durumda alıcısına karantinadan çıkartılarak iletilebilmelidir.

23) Karantinaya alınan mailler sistemin kendi üzerinde tutulabileceği gibi, harici bir NFS alanına da yazılabilmelidir.

24) Spam tespit edilemeyen şüpheli e-postlar için konu bölümüne uyarı eklenebilmelidir.

25) Kullanıcıların karantinaya düşen e-postları için bilgilendirme e-postaları otomatik olarak gönderilebilmelidir

26) Kullanıcılar karantinaya düşmüş e-postlarını bir web ara yüzü vasıtası ile karantinadan çıkarabilmelidir.

27) E-posta ayrı Güvenlik Sistemi, ayrı lisanslamaya gerek kalmadan;

71.1)Sistem herhangi bir e-posta sunucu gibi (MTA) çalışabilecek içeri ve dışarı yönde e-posta alıp verirken güvenlik denetimlerini gerçekleştirebilmelidir.

71.2)Sistem ihtiyaç duyulması halinde smtp sisteminde herhangi bir ayar değişikliği yapılmadan Layer 2 transparan olarak trafikte araya girebilecektir.

71.3)Sistem ihtiyaç duyulması halinde tam bir e-posta sunucu olarak çalışabilecek, gelen e-postalar üzerinde güvenlik denetimi yaparken aynı zamanda e-postları saklayacak ve kullanıcılara SMTP, POP3 ve IMAP protokol hizmetlerini verecektir. Bu çalışma modunda kullanıcılar tarafından web üzerinden e-posta erişimi de yapılabilir olacaktır.

28) E-posta güvenlik sistemi birden fazla e-posta alan adı ve birden fazla e-posta sunucusu ile çalışabilecektir.

29) Desteklenen e-posta domain sayısı adedi en az 70 olmalıdır.

30) E-posta koruma sisteminin depolama kapasitesi en az 2TB olmalıdır.

31) Sistemin saatte yönlendirebildiği e-posta sayısı en az 65.000 olmalıdır.

32) AV ve AntiSpam koruması devrede iken saatte tarayabildiği e-posta sayısı en az 50.000 olmalıdır.

33) Sistem aşağıdaki yöntemler ile yönetilebilmelidir:

77.1)Konsol port üzerinden

77.2)Web ara yüz üzerinden,

77.3)Command line üzerinden

34) Web ara yüzünden yönetim amaçlı güvenli erişim(https) yapılabilmelidir.
35) Yönetim için ayrı bir sistem gerekmemelidir.

36) Aynı model ikinci cihazın sisteme eklenmesi durumunda yönetimsel yedeklilikte sağlayabilecek mimaride olmalıdır.

37) SNMP desteği olmalıdır.

38) Web ara yüz üzerinden ve TFTP ile yazılım güncellemesi yapılabilmelidir.

39) E-posta koruma Sistemi kapsamlı kayıt (log) tutabilmeli ve raporlar üretebilmelidir.

40) Raporlar web ara yüzü üzerinden görülebileceği gibi aynı zamanda belirlenen aralıklarda otomatik oluşturulup e-posta ile gönderimi de sağlanabilmelidir.

41) Harici Syslog sunucularına kayıt (log) gönderebilecektir.

42) Teklif ile birlikte en az 3 yıl süre ile yazılım güncelleme ve 3 yıl süre ile AntiSpam ve AntiVirus/AntiMalware ile ilgili tüm güncellemeler için gerekli lisanslar verilmelidir.

43) Sistem üzerinde dışarı çıkmaması istenen e-posta adresleri otomatik olarak belirlenen başka adresler ile değiştirilebilmelidir.

44) En az %97 spam yakalama oranı olmalıdır. Bu durum bağımsız kuruluşlar tarafından (Yankee, Forrester, Gartner, Vbspam vb) belgelenmiş ve/veya test edilmiş olmalıdır. (bahsedilen raporlar teklifte ek olarak sunulacaktır.)

Loglama/Raporlama

Kayıt ve Raporlama Sistemi

45) Önerilen güvenlik duvarı sisteminin kayıt depolama ve takibini, raporlama işlemlerini gerçekleştirmek için aşağıda belirtilen şartlara uyan kayıt takip ve raporlama ürün/ürünleri alınacaktır.

2.1.1. Aşağıda belirtilen özellikler yönetim ve kayıt sistemlerinin ayrı veya tek bir sistem olarak önerilmesi durumunda da sağlanacaktır.

2.1.2. Önerilen sistem, saniyede en az 25 GB/Gün log kayıt alabilmelidir.

2.1.3. Log kayıt alanı olarak en az 10 TB depolama alanını desteklemelidir.

2.1.4. Önerilen kayıt ve raporlama sistemi, ağ güvenliği sistemi ile aynı marka olacaktır ve tam uyumlu bir şekilde entegre çalışabilecektir.

2.1.5. Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.

2.1.6. 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.

2.1.7. Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.

2.1.8. Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilmelidir.

2.1.9. Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.

2.1.10. 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.

2.1.11. 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.

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

2.1.13. pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.

2.1.14. Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek kayıtların yedekliliği sağlayabilmelidir.

2.2. Yukarıda belirtilen seçeneklerden hangisi ile teklif edilirse edilsin, teklif edilen sistemlerin en az 3 yıl yazılım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

5651 Log/Raporlama ve Hot Spot Yazılımı

Log/Raporlama Özellikleri :

1. Firewall Güvenlik Sistemi için kapsamlı logları tutabilecek ve raporlama yapabilecek Log/Raporlama yazılımı teklif edilmelidir.
2. Yazılımın Kurulacağı PC/Sunucu ve altyapısı kurum tarafından sağlanacaktır.
3. Log/Raporlama Yazılımı, MS Windows İşletim Sistemleri üzerinde çalışmalıdır. Desteklenen MS Windows İşletim Sistemleri belirtilmelidir. Log/Raporlama Yazılımı Sanal sistemler (Vmware, Hyper-V, Xen) üzerinde çalıştırılmak isteniyorsa MS Windows İşletim Sistemi Sanal Sistem üzerinde kurulu olmalıdır.
4. Log/Raporlama Yazılımının Log ve Disk kapasite sınırı olmamalıdır.
5. Log/Raporlama Yazılımı, Güvenlik Sistemi tarafından gönderilen Log Kayıtları üzerinden istenen kriterlere göre filtreleme yapabilmeli ve Güvenlik sistemi için en az 40 adet önceden tanımlanmış rapor üretebilmelidir.
6. Log/Raporlama Yazılımı lisanslama ile birden fazla aynı marka Güvenlik Sistemine ait log'ları merkezi olarak tutabilmeli ve raporlama yapabilmelidir.
7. Log/Raporlama Yazılımı; Trafik, Web, Uygulama, Email, Saldırı ve Olay gibi en az 6 farklı kategoride Rapor üretebilmelidir.Log/Raporlama Yazılımı, pdf formatında rapor üretebilmelidir.
8. Log/Raporlama Yazılımı, Log kayıtlarını ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek log yedekliliği sağlayabilmelidir. Log/Raporlama Yazılımı, Hata ve olay durumlarında belirtilen e-posta adresine bilgi verebilmelidir.
9. Log/Raporlama Yazılımı, 5651 sayılı kanunun uygulanmasına yönelik 'Internet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik' kapsamında, Log kayıtlarının doğruluğunu ve bütünlüğünü kendi üzerinde sağlamalıdır. Log/Raporlama Sistemi, 5651 sayılı kanun kapsamında Logların yedeklenmesi ve imzalanması, toplanan logların filtrelenmesi ve raporlanması işlevlerini yerine getirmelidir.
10. Log/Raporlama Yazılımı, 5651 sayılı kanunun uygulanmasına yönelik zaman damgası ve İmzalama için Kamu SM Entegrasyonu (Tübitak Kamu Sertifikasyon Merkezi) desteği sağlamalıdır. Kamu SM Zaman Damgası ve İmzalama hizmeti yazılımın içine gömülü olmalı bunun için ilave ücret ödenmemelidir. Log/Raporlama Yazılımı, Log kayıtlarına herhangi bir Zaman sunucudan alınan Zaman bilgisi ile Zaman damgası vurma ve Self-Signed Sertifika ile imzalama imkanını da sağlamalıdır.
11. Log/Raporlama Yazılımı, Güvenlik sistemine belirli sıklıkta SSH (Secure Shell) üzerinden bağlanarak IP/MAC adresi eşleştirme tablosunu alıp bu bilginin geçmişe yönelik kayıtlarını tutabilmelidir.

12. Lisanslama modeli, Log/Raporlama yazılımına Log gönderecek belirli Seri No'lu Güvenlik sistemleri için lisanslama şeklinde olmalıdır. Güvenlik sisteminin lisanslandığı süre boyunca Log/Raporlama sistemi bu sistemden log kabul edebilmelidir. Lisanslanan sürenin sona ermesinden sonra, eski döneme ait Log kayıtları üzerinde filtreleme ve raporlama imkanı devam etmelidir.
13. Log/Raporlama Yazılımı, Lisanslanan Güvenlik sisteminin konfigürasyon yedeklemesini istenen zamanlamaya göre SCP (Secure Copy Protocol) ile yapabilmeli ve bu konfigürasyon dosyaları şifreli bir veritabanı üzerinde tutulmalıdır.
14. Log/Raporlama Yazılımı, Güvenlik cihazına API (Application Programming Interface) üzerinden bağlanarak Güvenlik cihazının sağlamış olduğu altyapı ile anlık Network/Oturum vs. bilgileri takibi yapabilmelidir.
15. Log/Raporlama Yazılımı, Üzerinde tanımlı IP Kullanıcı Rehberi ile IP ve Kullanıcı adlarını eşleştirerek IP-Kullanıcı adı çözümlemesi yapabilmelidir. Log/Raporlama Yazılımı, Güvenlik sistemi üzerinden alınan Makina ismi veya LDAP protokolü ile sağlanan Kullanıcı adları ile IP-Kullanıcı adresi çözümlemesi yapabilmelidir.
16. Log/Raporlama Yazılımına Log gönderebilecek Seri No ile tanımlı Güvenlik Sistemleri, 3 yıl süre ile Log gönderebilecek şekilde lisanslanmalıdır.
17. Log/Raporlama Yazılımı; Güvenlik cihazının firmware versiyonundan bağımsız şekilde ve log formatında yapılan değişikliklerden etkilenmeyerek Log kaydı yapabilmelidir.

Hot Spot Özellikleri :

1. Log/Raporlama Yazılımı, Güvenlik sistemi ve aynı marka ve yönetilebilir wireless AP ile tam entegre olarak çalışacak Hot Spot yazılım özelliklerini desteklemelidir.
2. Hot Spot yazılımı, WiFi kullanıcı erişiminde SMS Doğrulama, TCKN Doğrulama, SMS+TCKN Doğrulama , Captive Portal özelliklerini desteklemelidir. Ek olarak mekanda bulunmayı doğrulayan gizli kelime (2FA) özelliğini desteklemelidir.
3. SMS Doğrulamada, SMS sağlayıcı olarak NetGSM, Vatan SMS ve Posta Güvercini sistemlerinden en az birini desteklemelidir.
4. Hotspot kullanıcıların anlık durumu (trafik, süre, bağlılık durumu vb.) Hotspot ekranından takip edilebilmeli ve gerektiğinde kullanıcının kimlik denetimi iptal edilebilmelidir.
5. Beyaz ve Kara Liste desteklenmeli ve gerektiğinde canlı ortam üzerinde tek tıklamayla herhangi bir kimlik kara listeye eklenebilmelidir.
6. Hotspot çerçevesinde kullanıcıların trafikleri ilgili kimlikleriyle loglara yansıtılmalıdır.
7. Geriye dönük tarihlere gidilerek hotspot bağlanan kullanıcı listesine erişilebilmelidir.
8. Hotspot karşılama ekranında çıkacak mesajlar özelleştirilebilmelidir.
9. Hot Spot dökümantasyonuna yazılıma ait Portal' dan erişilebilmelidir.
10. Hotspot özelliği, kullanılan Entegre Log/Raporlama yazılım lisansına dahil olmalıdır. Ek bir lisans gerektirmemelidir.

EK -1

TEKLİF VERİLECEK ÜRÜN LİSTESİ		
ÜRÜN	**ADET / KULANICI**	**BAKIM, ONARIM, DESTEK**