TRtest
Test ve Değerlendirme A.Ş.

AĞ GÜVENLİK DUVARI / FIREWALL ÜRÜN GRUBU KRİTERLERİ

No	Başlık/Soru	C (Giriş Seviye)	B (Orta Seviye)	A (Üst Seviye)
UG	**1- Ürün Güvenliği**			
UG_YA	**Yönetim Arayüzleri**			
UG_YA_WA	**1.1 Web Arayüzleri Zayıflık taraması**			
UG_YA_WA_1	Zararlı girdi kontrolü yapılıyor mu?	C		
UG_YA_WA_2	Çıktı Kodlama yapılıyor mu?	C		
UG_YA_WA_3	Kimlik Doğrulama kontrolü yapılıyor mu?	C		
UG_YA_WA_4	MultiFactor Authentication desteği var mı?		B	
UG_YA_WA_5	Parola yönetimi güvenliği sağlanıyor mu?	C		
UG_YA_WA_6	Karmaşıklık, Max uzunluk ve son kullanma süre periyodunun belirlenebileceği bir parola yönetim arayüzü var mı?		B	
UG_YA_WA_7	Erişim yönetimi ve yetkilendirme yapılıyor mu?	C		
UG_YA_WA_8	Yönetim arayüzüne erişim için izin verilen kaynaklar elle düzenlenen bir liste ile (IP adresine veya interface'e sahip ağlar için MAC adres listesi) yönetilebiliyor mu?		B	
UG_YA_WA_9	Kriptografi uygulamalarında zayıflığı bilinen algoritma kullanılmadığı teyit edildi mi?	C		
UG_YA_WA_10	Güvenli iletişim kanalları destekleniyor mu?	C		
UG_YA_WA_11	Veri tabanında hassas verilerin güvenliği sağlanıyor mu?		B	
UG_YA_WA_12	Dosya yönetiminde yetkilendirme ve güvenlik sağlanıyor mu?	C		
UG_YA_WA_13	Oturum yönetiminde yetki kontrolü yapılıyor mu?	C		
UG_YA_WA_14	Genel Kod API si varsa Genel kod (API) uygulamalarında kod güvenliği test ediliyor mu?	C		
UG_YA_K	**1.2 Konsol**			
UG_YA_K_SPM	**1.2.a Seri Port / Monitor**			
UG_YA_K_SPM_1	Zararlı girdi kontrolü yapılıyor mu?	C		
UG_YA_K_SPM_2	Kimlik Doğrulama, parola kaba kuvvet kontrolü yapılıyor mu?	C		
UG_YA_K_SPM_3	Parola yönetimi güvenliği sağlanıyor mu?	C		

UG_YA_K_SPM_4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	C		
UG_YA_K_AE	**1.2.b Ağ Üzerinden Erişim (SSH/Telnet vb.)**			
UG_YA_K_AE_1	Zararlı girdi kontrolü yapılıyor mu?	C		
UG_YA_K_AE_2	Kimlik Doğrulama, parola kaba kuvvet kontrolü yapılıyor mu?	C		
UG_YA_K_AE_3	Parola yönetimi güvenliği sağlanıyor mu?	C		
UG_YA_K_AE_4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	C		
UG_YA_K_AE_5	Güvenli iletişim kanalları destekleniyor mu?	C		
UG_YA_K_AE_6	Oturum yönetiminde zaman aşımı var mı?	C		
UG_YA_K_AE_7	Sistem yapılandırması doğru, güncel ve güvenli mi?	C		
UG_YA_D	**1.3. Diğer (Uygulama/API/Mobil varsa Yönetim)**			
UG_YA_D_1	Zararlı girdi kontrolü yapılıyor mu?	C		
UG_YA_D_2	Kimlik Doğrulama, parola kaba kuvvet kontrolü yapılıyor mu?	C		
UG_YA_D_3	Parola yönetimi güvenliği sağlanıyor mu?	C		
UG_YA_D_4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	C		
UG_YA_D_5	Güvenli iletişim kanalları destekleniyor mu?	C		
UG_YA_D_6	Sistem yapılandırması doğru, güncel ve güvenli mi?	C		
UG_YA_D_7	Oturum yönetiminde yetki kontrolü yapılıyor mu?	C		
UG_YA_D_8	Genel kod uygulamalarında kod güvenliği test ediliyor mu?	C		
UG_YA_D_9	Kullanıcının kişisel veri gizliliği (KVKK Uyumluluk) sağlanıyor mu?		B	
UG_YA_D_10	Bağlanmak için kullanılan veriler haricindeki kişisel veri içeren kayıtların operatör vb.. düşük seviye roller tarafından görüntülenmesi esnasında maskeleme teknikleri kullanılıyor mu?		B	
UG_ISS	**İşletim Sistemi ve Servisler**			
UG_ISS_1	Bilinen zayıflıklara karşı güvenlik önlemleri var mı?	C		
UG_ISS_2	Kimlik Doğrulama kontrolü yapılıyor mu?	C		
UG_ISS_3	Parola yönetimi güvenliği sağlanıyor mu?	C		
UG_ISS_4	Sistem yapılandırması doğru, güncel ve güvenli mi?	C		
UG_ISS_5	Yetki kontrolü yapılıyor mu?	C		
UG_ISS_6	DOS saldırılarına karşı koruma var mı?		B	

UG_ISS_7	SCAP uyumluluğu var mı?			A
UG_ISS_8	CISecurity uyumluluğu var mı?			A
UG_MT	**Masumiyet Testi**			
UG_MT_1	Teste tabi güvenlik duvarı herhangi bir dış noktaya şüpheli (açıklanamayan) paket/veri gönderiyor mu?	C		
UG_MT_2	Teste tabi güvenlik duvarı içeride görevi dışında açıklanamayan herhangi bir sisteme erişiyor mu?	C		
GFT	**2- Güvenlik Fonksiyon Testi**			
GFT_GD	**Güvenlik Duvarı**			
GFT_GD_1	IP Spoofing atak koruma özelliği destekliyor mu?	C		
GFT_GD_2	Port taramalara karşı koruma sağlıyor mu?	C		
GFT_GD_3	TCP Protokolü 3'lü el sıkışma kontrolü sağlıyor mu? (Asimetrik rota ile test edilebilir.)	C		
GFT_GD_4	TCP Split Handshake atağına karşı önlem alabiliyor mu?	C		
GFT_GD_5	TCP Syn anormallik engelleme özelliğini destekliyor mu? (Syn paketinde veri taşınması)		B	
GFT_GD_6	Parçalanmış paket kontrolü ve engellenmesi özelliğini destekliyor mu?	C		
GFT_GD_7	Arabirimler arası erişim denetimi sağlıyor mu?	C		
GFT_GD_8	Kural aksiyonları olarak ACCEPT/DENY/LOG özelliklerini destekliyor mu?	C		
GFT_GD_9	Dos/Ddos engelleme özelliğini destekliyor mu? (ICMP Flood, UDP Flood, Connection Flood, SYN, ACK, FIN Flood)		B	
GFT_GD_10	Kullanıcı/Grup/Zaman bazlı güvenlik duvarı kuralı yazımını destekliyor mu?		B	
GFT_GD_11	Oltalama saldırıları için veya botnet veya komuta kontrol merkezleri için kullanılan alan adı ve IP adreslerinden gelen erişim istekleri engelleme özelliğini destekliyor mu?	C		
GFT_GD_12	IP-MAC eşleme destekliyor mu?	C		
GFT_GD_13	Kural derleme sırasında izni olmayan bir erişimin paket iletimini engelliyor mu?	C		
GFT_GD_14	Uygulama tanıma/engelleme özelliğini destekliyor mu? (Ör. Dosya transferi, Sanal özel Ağ ve tünel uygulamaları, Vekil sunucu uygulamaları, Uzaktan erişim uygulamaları)		B	
GFT_GD_15	Uygulama tanıma sırasında paket kaçırmamayı destekliyor mu?			A
GFT_YT	**Yetkilendirme Testleri**			
GFT_YT_1	Active Directory, LDAP yetkilendirme/entegrasyon yöntemlerini destekliyor mu?		B	
GFT_SED	**SSH Erişimi Denetimi**			
GFT_SED_1	SSH üzerinden tünel erişimini engellemeyi destekliyor mu?			A

GFT_SED_2	SSH üzerinde dosya paylaşımını engellemeyi destekliyor mu?			A
GFT_STO	**Saldırı Tespit Ve Önleme (False/True Positive)**			
GFT_STO_1	Exploit saldırılarına karşı imza desteği var mı?		B	
GFT_STO_2	Phishing saldırılarına karşı imza desteği var mı?		B	
GFT_STO_3	Trojan/Malware saldırılarına karşı imza desteği var mı?		B	
GFT_STO_4	Brute Force saldırılarına karşı imza desteği var mı?		B	
GFT_STO_5	Code/Command Execution saldırılarına karşı imza desteği var mı?		B	
GFT_STO_6	Tarayıcı odaklı saldırılara karşı imza desteği var mı?		B	
GFT_STO_7	Protokol anormallik tespiti desteği var mı?		B	
GFT_STO_8	OWASP Top 10 saldırılarına karşı desteği var mı? (Injection, Broken Authentication, Sensitive Data Exposure, Xml External, Entities, Broken Access Control, Security Misconfiguration, XSS, Insecure Deserialization)		B	
GFT_WF	**Web Filtreleme (Http, Https)**			
GFT_WF_1	Kullanıcı/Grup/Zaman bazlı kural yazımını destekliyor mu?	C		
GFT_WF_2	URL, Alan adı, içerik, içerik tipi, eklenti, kelime, düzenli ifade(regex) engellemeyi destekliyor mu?	C		
GFT_WF_3	Kategori bazlı filtrelemeyi destekliyor mu?	C		
GFT_WF_4	Zayıf SSL algoritmalarını engelleme özelliğini destekliyor mu?			A
GFT_WF_5	XFF(x-forwarded-for) kontrolü sağlıyor mu?		B	
GFT_AV	**Anti-Virüs (http, https)**			
GFT_AV_1	Dosya uzantısına göre engelleme desteği var mı?	C		
GFT_AV_2	Eicar virüs dosyası ve içerik testi ile engelleme testini geçti mi?	C		
GFT_AV_3	Sıkıştırılmış dosya virüs testini geçti mi?	C		
GFT_AV_4	Ofis makro eklenti engelleme özelliğini destekliyor mu?	C		
GFT_AV_5	Wannacry için engelleme desteği sağlıyor mu?		B	
GFT_AV_6	Malware/Trojan türü zararlıların engellenmesini destekliyor mu?		B	
GFT_EG	**E posta Güvenliği**			
GFT_EG_1	Dosya uzantısına göre engelleme desteği var mı?		B	
GFT_EG_2	Eicar virüs dosyası ve içerik testi ile engelleme testini geçti mi?		B	

GFT_EG_3	Sıkıştırılmış dosya virüs testini geçti mi?		B	
GFT_EG_4	Ofis makro eklenti engelleme özelliğini destekliyor mu?		B	
GFT_EG_5	Wannacry için engelleme desteği sağlıyor mu?		B	
GFT_EG_6	Malware/Trojan türü zararlıların engellenmesini destekliyor mu?		B	
GFT_EG_7	Yetkilendirme olmadan eposta gönderen kullanıcının engellenmesini destekliyor mu?		B	
GFT_EG_8	Relay maillerin engellenmesini destekliyor mu?		B	
GFT_EG_9	E-posta seli saldırılarına karşı koruma/hafifletme desteği var mı?		B	
GFT_EG_10	Spam mail engellemeyi sağlıyor mu?		B	
GFT_EG_11	RBL Server desteği var mı?		B	
GFT_EG_12	Şüpheli alan adlarından gelen e-postaların kategori bazlı engellenmesini destekliyor mu? (Spam, Oltalama, Uzak Erişim, Peer-to-peer, Malware/Spyware, Dosya sunucuları, Vekil sunucu, Zombi ağı, Virüs içerikli siteler)			A
GFT_EG_13	Üreticinin kendi tehdit güncelleme servisi ile desteklediği bir kara liste (blacklist) desteği var mı ?		B	
GFT_DNS	**DNS (Alan adı sistemi)**			
GFT_DNS_1	DNS Sorgu tipine göre engelleme desteği var mı?			A
GFT_DNS_2	Kara Liste ve Beyaz Listeler oluşturmayı destekliyor mu?			A
GFT_DNS_3	Zararlı alan adlarına yapılan DNS sorgularını engellemeyi destekliyor mu? (Spam, Oltalama, Uzak Erişim, Peer-to-peer, Malware/Spyware, Dosya sunucuları, Vekil sunucu, Zombi ağı, Virüs içerikli siteler)			A
GFT_YST	**Yedeklilik Sistemi Testi**			
GFT_YST_1	Aktif-Pasif yedekli çalışmayı destekliyor mu?		B	
TO	**3- Temel Özellikler**			
TO_SO	**Sistem özellikleri**			
TO_SO_1	Cihazın web veya masaüstü arabirimlerinden yönetilebiliyor mu?	C		
TO_SO_2	SSH veya Seri Porttan Erişim Sağlanabiliyor mu?	C		
TO_SO_3	Disk yedekliliği açısından raid desteği var mı?			A
TO_SO_4	Yönetim arabirimi Türkçe ve İngilizce olmak üzere en az iki dil desteğini sağlıyor mu?	C		
TO_SO_5	Syslog ve SNMPv2,v3 desteği var mı?		B	
TO_SO_6	Web giriş şifresini console'den resetleyebilme özelliği var mı?	C		
TO_SO_7	Güncelleme desteği var mı?	C		

TO_SO_8	Konfig. bilgisini yedekleme ve geri dönme özelliği var mı?	C		
TO_SO_9	Yedekli kurulumu destekliyor mu? (NAT, Router, Bridge modlarda)		B	
TO_SO_10	IPv6 Ağ yapılandırma ve yönlendirme destekliyor mu?	C		
TO_SO_11	IPv6 NAT64, 6to4, DualStackTunnel destekliyor mu?			A
TO_SO_12	Sistem, IPS, URL filtering v.b. tanımlarını "Offline (Internet'e bağlanmadan) güncelleme yapabiliyor mu?			A
TO_SO_13	Cihaz yöneticileri için Sertifika bazlı kimlik doğrulama yapabiliyor mu ?		B	
TO_SO_14	Yönetim arayüzü için Rol bazlı yetkilendirme yapılıyor mu ? Modül ve fonksiyon bazlı özel roller eklenebiliyor mu? (Ör. Auditor, Monitor, Network Admin, Operator vb.)	C		
TO_SO_15	Cihaz yöneticilerinin yapmış olduğu işlemler özelinde detaylı audit log tutabiliyor mu ? (eski değer, yeni değer, ilgili kişi ip adresi tarih ve saat vb.)	C		
TO_SO_16	SSL Inspection yapabiliyor mu ?	C		
TO_KY	**Kullanıcı yönetimi ve entegrasyon özellikleri**			
TO_KY_1	Yerel kullanıcı ve grup eklenebiliyor mu?	C		
TO_KY_2	Microsoft Active Directory NTLM veya Kerberos entegrasyonu destekleniyor mu?		B	
TO_KY_3	Çoklu LDAP entegrasyonu desteği var mı?		B	
TO_KY_4	Kullanıcılar için radius doğrulama servisi var mıdır ?		B	
TO_KY_5	Güvenlik duvarında kullanıcı/grup kullanılabiliyor mu?		B	
TO_KY_6	Uygulama kontrolünde kullanıcı/grup kullanılabiliyor mu?		B	
TO_KY_7	Web filtrede kullanıcı/grup kullanılabiliyor mu?	C		
TO_KY_8	Kullanıcı giriş portalında kullanıcı/grup kullanılabiliyor mu?	C		
TO_KY_9	SSLVPN'de kullanıcı/grup kullanılabiliyor mu?		B	
TO_KY_10	IDS-IPS gibi yerlerde kullanıcı/grup kullanılabiliyor mu?		B	
TO_KY_11	Kullanıcı/Grup için kullanım zamanı ve veri indirme kotası ayarlanabiliyor mu?		B	
TO_AO	**Ağ özellikleri**			
TO_AO_1	10/100/1000 fiziksel arabirim ve PPPOE, VLAN, BRIDGE, LACP(BOND), LOOPBACK yazılımsal arabirim desteği var mı?	C		
TO_AO_2	10 Gigabit fiziksel arabirim desteği var mı?			A
TO_AO_3	3G/4G Internet aygıtları yazılımsal arabirim desteği var mı?		B	
TO_AO_4	Tek noktaya (Unicast), Çok noktaya (Multicast) yönlendirme özellikleri var mı?		B	

TO_AO_5	Politika tabanlı ve dinamik(bgp, ospf vs.) yönlendirme özellikleri var mı?		B	
TO_AO_6	NAT, Router mod desteği var mı?	C		
TO_AO_7	Bridge mod desteği var mı?		B	
TO_AO_8	LLDP(Link Layer Discovery Protocol) özelliği var mı?			A
TO_AO_9	DHCP servisi var mıdır ve her arabirimi özelleştirebiliyor mu?	C		
TO_AO_10	DNS önbellek servisi var mı?	C		
TO_AO_11	Çoklu internet hattı desteği var mı?	C		
TO_AO_12	Kural tabanlı internet yük dengeleme ve hata kontrolü desteği ile otomatik internet hattı değişimi yapabiliyor mu?		B	
TO_AO_13	Farklı tip hatları (xDSL, 3G/4.5G, ME) birleştirme yapabiliyor mu?		B	
TO_AO_14	Her bir ethernet portu özelleştirilebiliyor mu?	C		
TO_SAO	**Sanal özel ağ özellikleri**			
TO_SAO_1	Güvenli bağlantı için VPN (L2TP over IPSec, SSLVPN) desteği var mı?	C		
TO_SAO_2	Noktadan-Noktaya IPSec VPN (IKEv1-v2) desteği var mı?	C		
TO_SAO_3	IPSec, SSLVPN ve L2TP over IPSec VPN türleri en az AES şifreleme yöntemlerini ve SHA doğrulama yöntemlerini destekliyor mu?	C		
TO_GD	**Güvenlik duvarı özellikleri**			
TO_GD_1	Kural yazılırken oturum kontrollü/kontrolsüz yazılabiliyor mu?	C		
TO_GD_2	Parçalanmış paket kontrolü ve engellemesi var mı?	C		
TO_GD_3	IP, ağ adresi, IP aralığı gibi nesneler kullanılarak kural yazılabiliyor mu?	C		
TO_GD_4	Kullanıcı/Grup kullanılarak kural yazılabiliyor mu?		B	
TO_GD_5	Kural aksiyonu olarak izin ver/engelle/kayıt(log) seçeneklerini barındırıyor mu?	C		
TO_GD_6	NAT-PAT destekleniyor mu?	C		
TO_GD_7	IP-MAC eşleştirme destekleniyor mu?	C		
TO_GD_8	L7 Uygulama tanımlı kural yazımını destekliyor mu?		B	
TO_GD_9	SSL protokolü ile çalışan uygulamaları da tanıyıp aksiyon alabiliyor mu?			A
TO_GD_10	IP spoofing saldırı koruma özelliği var mıdır ?	C		
TO_GD_11	TCPSYN paketlerindeki anormalik tespiti yapabiliyor mu?		B	
TO_GD_12	Temel DoS/DDoS koruması(minimum SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood, Connection Flood) sağlıyor mu?		B	

TO_GD_13	DDoS korumaya(minimum SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood, Connection Flood) özel politika bazlı kural yazabilmeye imkan tanıyor mu?		B	
TO_GD_14	Zaman tanımlı kural yazımını destekliyor mu?	C		
TO_GD_15	Dışarıdan tespit edilmemesi için management portlar kapatılabiliyor mu ?	C		
TO_GD_16	Politika bazlı yönlendirme desteği var mıdır?	C		
TO_GD_17	DHCP servisinde tanımlanan MAC-IP adreslerinin dışında IP almasını engellenebiliyor mu?	C		
TO_GD_18	Port, uygulama ve IP bazında QoS servisi destekliyor mu?		B	
TO_SSH	**SSH derin inceleme özellikleri**			
TO_SSH_1	SSH tünel engellenebiliyor mu?			A
TO_SSH_2	SSH protokolü üzerinden dosya transferlerini kapatabiliyor mu?			A
TO_WF	**Web filtre özellikleri**			
TO_WF_1	URL, alan adı, içerik filtreleme, dosya uzantısı, regex ile fitreleme desteği var mı?	C		
TO_WF_2	Kategori bazlı filtreleme yapılabiliyor mu?	C		
TO_WF_3	Web içeriği için antivirüs desteği var mıdır?	C		
TO_WF_4	Gruplara zaman tanımlaması yapılıyor mu?	C		
TO_WF_5	Birden fazla Web filtre grubu ile farklı politikaları(filtresiz,filtreli) destekleniyor mu?	C		
TO_WF_6	Kullanıcı/grup, IP, ağ adresi, IP aralığı gibi nesneler kullanılarak kural yazılabiliyor mu?	C		
TO_WF_7	HTTPS alan adı veya içerik bazlı filtreleme ve virüs taraması yapabiliyor mu?	C		
TO_WF_8	Güvenli bağlantı için kara liste ve beyaz liste tanımlanabiliyor mu? Bu listeler otomatik güncellenebiliyor mu ?	C		
TO_DNS	**DNS filtreleme özellikleri**			
TO_DNS_1	DNS üzerinden kategori bazlı filtreleme yapılabiliyor mu?			A
TO_DNS_2	DNS sorgularını belirtilen farklı bir IP adresini çözerek yönlendirebiliyor mu?			A
TO_STO	**Saldırı tespit ve önleme özellikleri**			
TO_STO_1	Ağ tabanlı Saldırı Tespit ve Engelleme Sistemleri (NIDS/NIPS) var mı?		B	
TO_STO_2	Ethernet arabirimi ve/veya kural tabanlı çalışabiliyor mu?		B	
TO_STO_3	İmza tabanlı atak tespiti yapabiliyor mu?		B	
TO_STO_4	Kullanıcı/grup, IP, ağ adresi gibi nesneler kullanılarak kurallar yazılabiliyor mu?		B	
TO_STO_5	Protokol ve trafik anormallik tespiti yapabiliyor mu?			A

TO_EPG	**E-Posta güvenliği özellikleri**			
TO_EPG_1	E-Posta için Antispam ve antivirüs desteği var mıdır?		B	
TO_EPG_2	E-posta güvenliği için kara liste ve beyaz liste oluşturulabiliyor mu?		B	
TO_EPG_3	Spam mailleri karantinaya atabiliyor mu? Karantina mail yönetimini destekliyor mu?		B	
TO_EPG_4	Spam veya şüpheli mailleri içerik ve alan adı kategorisine göre engelleyebiliyor mu?		B	
TO_EPG_5	Real Time Blacklist (RBL) Filtreleme yapabiliyor mu?		B	
TO_KGP	**Kullanıcı Giriş Portalı (Hotspot/Captive Portal) özellikleri**			
TO_KGP_1	Hotspot bağlantı için SMS ile doğrulama yapabiliyor mu?		B	
TO_KGP_2	Hotspot bağlantı için Özel SMS API bağlantısı ile doğrulama yapabiliyor mu?		B	
TO_KGP_3	Hotspot bağlantı için T.C. Kimlik ile doğrulama yapabiliyor mu?		B	
TO_KGP_4	Hotspot bağlantı için LDAP ile doğrulama yapabiliyor mu?		B	
TO_KGP_5	Hotspot bağlantı için Lokal kullanıcı ile doğrulama yapabiliyor mu?	C		
TO_KGP_6	Hotspot bağlantı için 3'üncü parti veri tabanları ile doğrulama yapabiliyor mu?			A
TO_KGP_7	Hotspot da farklı dil desteği var mı ve farklı profil oluşturulabiliyor mu?	C		
TO_KGP_8	Kullanıcılarına zaman ve veri kotası uygulanabiliyor mu?		B	
TO_KGP_9	Müşteriye göre hotspot ekranı özelleştirilebiliyor mu?		B	
TO_KG	**Kayıt Altına Alma ve Görüntüleme Özellikleri**			
TO_KG_1	Kanuna uygun loglama yapıp 5651 ve KVKK kapsamında kayıt tutabiliyor mu? Zaman damgası ile (T.C. e-imza kanununa göre geçerli bir sertifika sağlayıcı ile kayıtları en az günlük olarak) mühürleyebiliyor mu ?	C		
TO_KG_2	Log kayıtlarında kullanıcı bilgisi, kaynak-hedef IP bilgisi değerleri var mı?	C		
TO_KG_3	Log kayıtlarında uygulama adı ve kural numarası gibi değerler var mı?		B	
TO_KG_4	Oturum başlangıç-bitiş zamanları, paket ve veri miktarı ile ilgili kayıtlar tutuluyor mu?			A
TO_KG_5	İmzalanmış log kayıtlarını yasal zorunluluk olan en az 2 yıl saklayabiliyor mu?	C		
TO_KG_6	Log kayıtları lokal diskin dışında uzak sistemlere gönderilebiliyor mu? (ftp, scp, smb, syslog)		B	
TO_KG_7	Oluşan log kayıtları canlı incelenebiliyor mu?	C		
TO_KG_8	Oluşan log kayıtları geriye doğru incelenebiliyor mu?		B	
TO_R	**Raporlama Özellikleri**			

TO_R_1	Default şablonlar ile hızlı rapor alınabiliyor mu?	C		
TO_R_2	Raporların çıktısını özelleştirebiliyor muyuz?		B	
TO_R_3	Yönetim, Güvenlik duvarı, web filtre, DHCP, hot spot, oturum geçmişi, anti-virüs/anti-spam, IPS kayıtları ile ilgili raporlar alınabiliyor mu?		B	
TO_I	**İzleme Özellikleri**			
TO_I_1	Dashboard ekranı üzerinde görsel özelleştirme yapılabiliyor mu?		B	
TO_I_2	Dashboard ekranında veya monitoring yazılımlarında ağ trafiği canlı ve grafiksel izlenebiliyor mu?	C		
TO_I_3	IPSec, SSLVPN, Hot spot gibi modüllerin bağlı kullanıcılarının bağlantı durumları izlenebiliyor mu?	C		
TO_I_4	Dashboard ekranında donanım kaynakları izlenebiliyor mu?	C		
TO_UD	**Ürün Dokümantasyonu**			
TO_UD_1	Türkçe ve İngilizce doküman desteği var mıdır?	C		
TO_UD_2	Ürün kutusu içerisinde hızlı kurulum, ürün özellikleri ve saklama koşullarını gösteren yazılı veya elektronik yönetici el kitabı yer alıyor mu?	C		
TO_UD_3	Üreticinin ürüne ilişkin forum/bilgi deposu ve çağrı sistemi web sayfaları var mı?	C		
TO_UD_4	Üretici web sayfasında sık sorulan sorular veya ürünle alakalı makale, blog sayfası var mıdır ?		B	
TO_UD_5	Youtube veya benzeri video paylaşım sitelerinde ürünün temel özellikleri ile ilgili kurulum veya yapılandırma videoları var mıdır ?			A
TO_UD_6	Ürünün üretici tarafından yayınlanan güncellemelerine ilişkin sürüm notları ile ilgili doküman müşteriler tarafından çevrimiçi erişilebiliyor mu?		B	
PK	**4. Performans / Kapasite**			
PK_1	Ürün üretici tarafından beyan edilen performans kriterlerini sağlıyor mu?	C		
PK_2	Üretici tarafından test ortamı ve test edilecek ürünün modeli belirtilmiş mi?	C		
PK_3	**Ürüne ilişkin aşağıdaki testler yapılarak performans raporu alınmalıdır.**			
PK_3_1	**Maksimum Kapasite**			
PK_3_1_1	Maksimum Eşzamanlı Teorik TCP Bağlantısı	C		
PK_3_1_2	Saniyedeki maksimum Yeni TCP Bağlantısı	C		
PK_3_1_3	Saniyedeki maksimum HTTP Bağlantısı	C		
PK_3_1_4	Saniyedeki maksimum HTTP Hareketi (ing: transaction)	C		
PK_3_1_5	Maksimum eşzamanlı IPSec bağlantısı.	C		
PK_3_1_6	Maksimum eşzamanlı SSLVPN bağlantısı	C		

PK_3_2	**Sistem çıktısı (*Throughput*) Performansı**			
PK_3_2_1	· Farklı Çerçeve Boylarında (1518 byte, 512 byte, 64 byte traffic, IMIX) Güvenlik Duvarı (Mbps olarak başarı ile taşınabilen maksimum hızın(ing: rate) ölçülmesi amaçlanır.)	C		
PK_3_2_2	· Güvenlik Duvarı ve HTTP Proxy olarak (antivirüs ile birlikte ve antivirüs olmadan)	C		
PK_3_2_3	· Güvenlik Duvarı ve HTTPS olarak	C		
PK_3_2_4	· Güvenlik Duvarı ve IPS olarak	C		
PK_3_2_5	· Güvenlik Duvarı, HTTP ve IPS olarak	C		
PK_3_2_6	· UTM, Next Generation (eğer uygulanabilirse)	C		
PK_3_2_7	· IPSec site-to-site throughput test	C		
PK_3_3	**Ham Paket İşleme Performansı (UDP Throughput)**			
PK_3_3_1	· 64 Byte Paketler	C		
PK_3_3_2	· 128 Byte Paketler	C		
PK_3_3_3	· 256 Byte Paketler	C		
PK_3_3_4	· 512 Byte Paketler	C		
PK_3_3_5	· 1024 Byte Paketler	C		
PK_3_3_6	· 1514 Byte Paketler	C		
PK_3_3_7	· Jumbo Paketler	C		
PK_3_4	**Gecikme (Latency)**			
PK_3_4_1	· 64 Byte Çerçeveler	C		
PK_3_4_2	· 128 Byte Çerçeveler	C		
PK_3_4_3	· 256 Byte Paketler	C		
PK_3_4_4	· 512 Byte Paketler	C		
PK_3_4_5	· 1024 Byte Paketler	C		
PK_3_4_6	· 1514 Byte Paketler	C		
PK_3_4_7	· Jumbo Paketler	C		
PK_3_5	**SSL/TLS Performance** - HTTPS Filtreleme Performansı	C		
PK_3_6	**Karışık Trafik**			

PK_3_6_1	· Bütün UTM fonksiyonlarının aynı anda açık olduğu durumda ve karışık trafik üretilerek performans testi yapılabilir. (Güvenlik Duvarı, NGFW) o %70 HTTPS and %30 HTTP	C		
PK_3_6_2	· Özel sektör dikeylerini ve / veya kullanım durumlarını temsil eden trafik karışımları geliştirilmelidir.	C		
PK_3_1	**Esneklik (Resiliency)**			
PK_3_1_1	· Yüksek Erişilebilirlik **High Availability (Varsa belirtilmelidir)**	C		
PK_3_1_2	· By Pass Desteği (Varsa Belirtilmelidir.)	C		
PK_GDP	**Güvenlik Duvarının Performası**			
PK_GDP_1	Güvenlik Duvarı, trafiği ayrıntı seviyesine göre öncelik sırasına koyabiliyor mu?		B	
PK_GDP_2	Garantili bant genişliği ile VOIP ve Video konferans trafiğini önceliklendirebiliyor mu?		B	
PK_GDP_3	Güvenlik duvarı, performans istatistiklerini, paket kayıplarını, sistem kaynakları kullanımını gösteriyor mu?		B	
RU	**5- REGÜLASYONLARA UYUM**			
RU_TCK	**TCK 5651/5070**			
RU_TCK_1	Kanunun kayıt tutma hükümlerine uyumluluğu var mı?	C		
RU_TCK_2	Kanunun zaman damgası kriterlerine göre 5070 sayılı kanun tarafından yetkilendirilmiş bir zaman damgası kullanımını destekliyor mu?	C		
RU_TCK_3	Kanunun katalog suçların engellenmesi hükümlerine uyumluluğu var mı?	C		
RU_TCK_4	Kanunun refere ettiği yönetmelik ve benzeri mevzuat ile uyumluluğu var mı?	C		
RU_KVKK	**KVKK**			
RU_KVKK_1	Ürün hotspot kullanımı sırasında Kişisel Verilerin Kullanımı ile ilgili sözleşme bilgilendirme ve onay alma sistemini destekliyor mu?	C		
RU_KVKK_2	Ürün kişisel verileri, sözleşme ve bilgilendirmelere aykırı şekilde, cihaz dışına transfer etmediğini onaylıyor mu?		B	
RU_KVKK_3	Ürün kişisel verileri cihaz dışına transfer ediyorsa buna baz olacak kişisel verilerin kullanımı sözleşmesi bilgilendirme ve onayını aldığını kanıtlayabiliyor mu?	C		