



FIREWALL ÜRÜN GRUBU KRİTERLERİ

EPATİ BİLİŞİM TEKNOLOJİLERİ

SAN. VE TİC. LTD. ŞTİ.

ANTİKOR V2.0

09.02.2021

YÖNETİCİ ÖZETİ

TRTEST TEST VE DEĞERLENDİRME A.Ş.
İvedik O.S.B. Mahallesi 2224. Cadde No:1/250
Yenimahalle/ ANKARA
Ulus V.D. 859 064 7995 Tic.Sic.No:15473
Mersis No: 0859 0647 9950 0001


Ankara Teknopark
İvedik OSB Mahallesi 2224.Cadde 1/250 C Blok Kat:13
Yenimahalle /ANKARA

Bilgi için: Büşra Nur YÜZER,
Telefon No:0 850 551 00 00 /25

Telif ve Gizlilik Notu

Bu doküman TRTEST tarafından belirtilen kuruluşa özel olarak hazırlanmıştır.

Bu dokümanın hiçbir bölümü TRTEST 'in yazılı izni olmaksızın değiştirilemez, doküman sahibi haricinde herhangi bir kişi ya da kuruluş ile paylaşamaz.

Bu dokümanın içeriği TRTEST 'in fikri malıdır. Sözleşmelerle belirlenmiş kullanıcı hakları dışında, bu dokümanın tamamının veya bir bölümünün herhangi bir şekilde TRTEST 'in izni olmaksızın çoğaltılması, başkalarına verilmesi ve kullanımı ile ilgili her türlü uygulama yasaktır.

Kontrollü dağıtımı yapılan kopyalar dışındakilerin güncel olmasını sağlamak kullanıcı sorumluluğundadır.

Bu dokümanın üretiminde kullanılan yöntemler, dokümanın biçimi, içeriği, elde edilen bulgulara ilişkin açıklama ve öneriler TRTEST 'in entelektüel varlığıdır.

Bu dokümanın kontrollü olarak güncel hali TRTEST intranetinde yer alır.

© 2020 – TRTEST A.Ş. Tüm hakları saklıdır.

TRTEST TEST VE DEĞERLENDİRME A.Ş.
İvedik O.S.B. Mahallesi 2224. Cadde No:1 / 250
Yenimahalle/ ANKARA
Ulus V.D. 859 064 7995 Tic.Sic.No: 295473
Mersis No: 0803004709500004
BN

Ankara Teknopark
İvedik OSB Mahallesi 2224.Cadde 1/250 C Blok Kat:13
Yenimahalle /ANKARA

Bilgi için: Büşra Nur YÜZER,
Telefon No:0 850 551 00 00 /25

TRTEST     iştirakidir.

İÇİNDEKİLER

1 Yönetici Özeti.....	1
1.1 Genel Bilgiler.....	1
1.2 Test Metodolojisi.....	1
1.3 Özet Test Sonuçları.....	3
2 Test Durumu.....	14

TRTEST TEST VE DEĞERLENDİRME A.Ş.
İvedik O.S.B. Mahallesi 2224. Cadde No:1 /250
Yenimahalle/ ANKARA
Ulus V.D. 859 064 7995 Tic. Sic. No: 276173
Mersis No: 0819 0047 9950 0004

1 Yönetici Özeti:

1.1 Genel Bilgiler:

Bu raporda bahsi geçen “firma” deyimini EPATİ BİLİŞİM TEKNOLOJİLERİ SAN. VE TİC. LTD. ŞTİ. ‘yi ifade eder. Testler Innovera Bilişim Teknolojileri A.Ş tarafından gerçekleştirilmiş, Test süreci TRTEST Test ve Değerlendirme A.Ş. gözetiminde yapılmıştır

FIREWALL ürün grubu TRTEST-TSGK-FIREWALL-01 kriterine göre. EPATİ BİLİŞİM TEKNOLOJİLERİ SAN. VE TİC. LTD. ŞTİ firması Antikor v2.0 ürünü testlerine “firma” teknik ekibi tarafından gerekli test ortamı oluşturulmuştur.

Testler TRTEST Test ve Değerlendirme A.Ş lokasyonunda test sunucusu ile konumlandırılan test cihazları üzerinde gerçekleştirilmiştir.

Testlere 9 Haziran 2020 tarihinde başlamış, 25 Ağustos 2020 tarihinde test raporu hazırlanmıştır. Penetrasyon ve güvenlik testleri Innovera’dan bir kişinin katılımı ile, fonksiyon testleri Innovera’dan bir kişinin katılımı ile gerçekleştirilmiştir. Test süreci TR-Test gözetiminde yapılmıştır.

Retest kapsamındaki çalışma 6 Ekim 2020 tarihinde başlamış, 9 Kasım tarihinde tamamlanmıştır. Penetrasyon ve güvenlik testleri Innovera pentest ekibinden bir kişi, fonksiyon testleri Innovera’dan iki kişinin katılımı, üretici tarafından bir kişinin katılımı ile gerçekleştirilmiştir. Re-test süreci TR-Test gözetiminde yapılmıştır.

Testler esnasında herhangi bir zorlukla karşılaşılmamış olup firma personellerinin ilgi ve alakası test ekiplerince minnetle karşılanmıştır.

1.2 Test Metodolojisi:

Tüm test maddeleri için öncesinde belirlenen test metodolojisine göre firewall üzerinde kontroller yapılmış, firewall üzerinden geçen trafik üretilmiş ve sonuçları kayıt altına alınmıştır. Kayıt altına alma işlemi ekran görüntüsü ve ilgili ayarın yapılandırma dosyasının kaydedilmesi şeklinde gerçekleştirilmiştir. Tüm ekran görüntüleri test edilen maddenin numarası ile başlamakta, test maddesinin adını içermektedir.

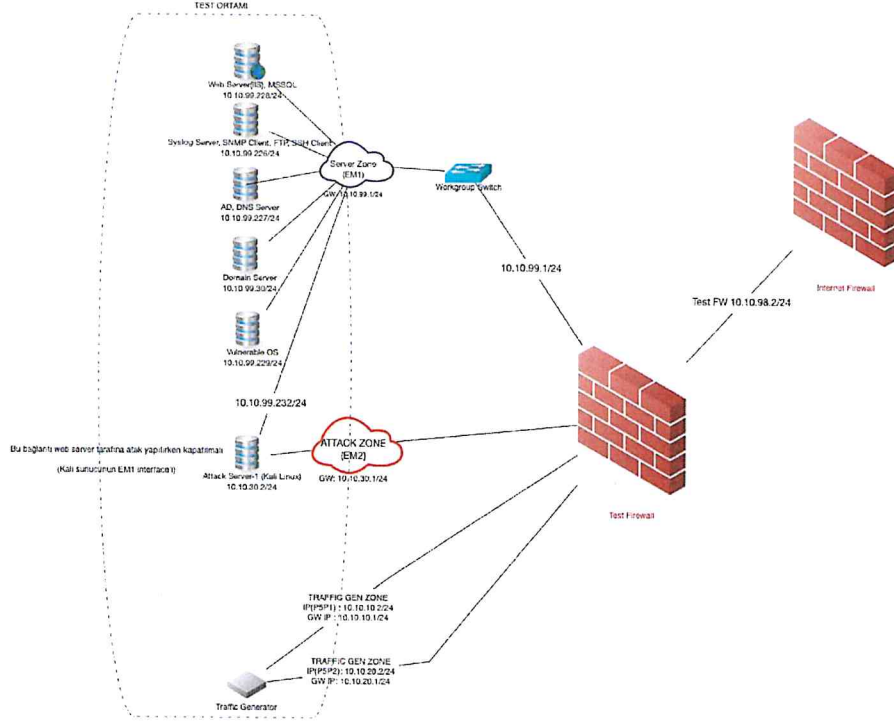
Test Ortamı Topolojisi

TRTEST TEST VE DEĞERLENDİRME A.Ş.
İvedik O.S.B. Mahallesi 2224. Cadde No:1 / 250
Yenimahalle/ ANKARA
Ulus V.D. 850 551 7995 Tic.Sic.No: 274573
Mersis No: 0803001799500004

Ankara Teknopark
İvedik OSB Mahallesi 2224.Cadde 1/250 C Blok Kat:13
Yenimahalle /ANKARA

Bilgi için: Büşra Nur YÜZER,
Telefon No:0 850 551 00 00 /25

TRTEST     iştirakidir.



Sunucu bilgileri,

Sunucu	Amacı	Network Bilgileri
1. Centos Minimal	Cisco-Trex	EM1: 10.10.99.99/24 MLNX1: 10.10.10.2 MLNX2: 10.10.20.2
2. Centos (GUI)	Syslog 514 SNMP 161 FTP 21	EM1: 10.10.99.226/24
3. Windows Server	Active Directory DNS Radius Hmail	EM1: 10.10.99.227/24
4. Windows Server	IIS MSSQL	EM1: 10.10.99.228/24
5. Linux Vulnerable OS		EM1: 10.10.99.229/24
6. Kali Linux	Atak araçları	EM1: 10.10.99.232/24 EM2: 10.10.30.232/24
7. Win SRV		EM1:10.10.99.225/24
8. Vulnerable Win8		EM1:10.10.99.111/24
ESXi Host		Management: 10.10.99.252

TRTEST TEST VE DEĞERLENDİRME A.Ş.
İvedik O.S.B. Mahallesi 2224. Cadde No:1/250
Yenimahalle/ ANKARA
Ulusal M.D. 653/064 7096 Tic.Sic.No:415473
Mersis: 081700304799500001

Ankara Teknopark
İvedik OSB Mahallesi 2224.Cadde 1/250 C Blok Kat:13
Yenimahalle /ANKARA

Bilgi için: Büşra Nur YÜZER,
Telefon No:0 850 551 00 00 /25

TRTEST iştirakidir.

1.3 Özet Test Sonuçları:

No	Başlık/Soru	C	B	A	DURUM
	1- Ürün Güvenliği				
	Yönetim Arayüzleri				
UG_WA	1.1 Web Arayüzleri Zayıflık taraması				
UG_WA.1	Zararlı girdi kontrolü yapılıyor mu?	1			BAŞARILI
UG_WA.2	Çıktı Kodlama yapılıyor mu?	1			BAŞARILI
UG_WA.3	Kimlik Doğrulama kontrolü yapılıyor mu?	1			BAŞARILI
UG_WA.4	MultiFactor Authentication desteği var mı?		1		BAŞARILI
UG_WA.5	Parola yönetimi güvenliği sağlanıyor mu?	1			BAŞARILI
UG_WA.6	Karmaşıklık, Max uzunluk ve son kullanma süre periyodunun belirlenebileceği bir parola yönetim arayüzü var mı?		1		BAŞARILI
UG_WA.7	Erişim yönetimi ve yetkilendirme yapılıyor mu?	1			BAŞARILI
UG_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?		1		BAŞARILI
UG_WA.9	Kriptografi uygulamalarında zayıflığı bilinen algoritma kullanılmadığı teyit edildi mi?	1			BAŞARILI
UG_WA.10	Güvenli iletişim kanalları destekleniyor mu?	1			BAŞARILI
UG_WA.11	Veri tabanında hassas verilerin güvenliği sağlanıyor mu?		1		BAŞARILI
UG_WA.12	Dosya yönetiminde yetkilendirme ve güvenlik sağlanıyor mu?	1			BAŞARILI
UG_WA.13	Oturum yönetiminde yetki kontrolü yapılıyor mu?	1			BAŞARILI
UG_WA.14	Genel Kod API si varsa Genel kod (API) uygulamalarında kod güvenliği test ediliyor mu?	1			ÖZELLİK BULUNMUYOR
	1.2 Konsol				
UG_SPM	1.2.a Seri Port/Monitor				
UG_SPM.1	Zararlı girdi kontrolü yapılıyor mu?	1			BAŞARILI
UG_SPM.2	Kimlik Doğrulama, parola kaba kuvvet kontrolü yapılıyor mu?	1			BAŞARILI
UG_SPM.3	Parola yönetimi güvenliği sağlanıyor mu?	1			BAŞARILI
UG_SPM.4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	1			BAŞARILI
UG_AE	1.2.b Ağ Üzerinden Erişim (SSH/Telnet Vb)				
UG_AE.1	Zararlı girdi kontrolü yapılıyor mu?	1			BAŞARILI
UG_AE.2	Kimlik Doğrulama, parola kaba kuvvet kontrolü yapılıyor mu?	1			BAŞARILI

UG_AE.3	Parola yönetimi güvenliği sağlanıyor mu?	1		BAŞARILI
UG_AE.4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	1		BAŞARILI
UG_AE.5	Güvenli iletişim kanalları destekleniyor mu?	1		BAŞARILI
UG_AE.6	Oturum yönetiminde zaman aşımı var mı?	1		BAŞARILI
UG_AE.7	Sistem yapılandırması doğru, güncel ve güvenli mi?	1		BAŞARILI
UG_D	1.3. Diğer (Uygulama/API/Mobil varsa Yönetim)	1		
UG_D.1	Zararlı girdi kontrolü yapılıyor mu?	1		Özellik Bulunmuy or
UG_D.2	Kimlik Doğrulama, parola kaba kuvvet kontrolü yapılıyor mu?	1		Özellik Bulunmuyo r
UG_D.3	Parola yönetimi güvenliği sağlanıyor mu?	1		Özellik Bulunmuyo r
UG_D.4	Erişim yönetimi ve yetkilendirme yapılıyor mu?	1		Özellik Bulunmuyo r
UG_D.5	Güvenli iletişim kanalları destekleniyor mu?	1		Özellik Bulunmuyo r
UG_D.6	Sistem yapılandırması doğru, güncel ve güvenli mi?	1		Özellik Bulunmuyo r
UG_D.7	Oturum yönetiminde yetki kontrolü yapılıyor mu?	1		Özellik Bulunmuyo r
UG_D.8	Genel kod uygulamalarında kod güvenliği test ediliyor mu?	1		Özellik Bulunmuyo r
UG_D.9	Kullanıcının kişisel veri gizliliği (KVKK Uyumluluk) sağlanıyor mu?		1	Özellik Bulunmuyo r
UG_D.10	Bağlanmak için kullanılan veriler haricindeki kişisel veri içeren kayıtların operatör vb. düşük seviye roller tarafından görüntülenmesi esnasında maskeleyme teknikleri kullanılıyor mu?		1	Özellik Bulunmuyo r
UG_İSS	İşletim Sistemi ve Servisler	1		
UG_İSS.1	Bilinen zayıflıklara karşı güvenlik önlemleri var mı?	1		BAŞARILI
UG_İSS.2	Kimlik Doğrulama kontrolü yapılıyor mu?	1		BAŞARILI
UG_İSS.3	Parola yönetimi güvenliği sağlanıyor mu?	1		BAŞARILI
UG_İSS.4	Sistem yapılandırması doğru, güncel ve güvenli mi?	1		BAŞARILI
UG_İSS.5	Yetki kontrolü yapılıyor mu?	1		BAŞARILI
UG_İSS.6	DOS saldırılarına karşı koruma var mı?		1	BAŞARILI
UG_İSS.7	SCAP uyumluluğu var mı?			1 BAŞARILI
UG_İSS.8	CISecurity uyumluluğu var mı?			1 BAŞARILI

UG_MT	Masumiyet Testi				
UG_MT.1	Teste tabi güvenlik duvarı herhangi bir dış noktaya şüpheli (açıklanamayan) paket/veri gönderiyor mu?	1			BAŞARILI
UG_MT.2	Teste tabi güvenlik duvarı içeride görevi dışında açıklanamayan herhangi bir sisteme erişiyor mu?	1			BAŞARILI
	2- Güvenlik Fonksiyon Testi				
GF_GD	Güvenlik Duvarı				
GF_GD.1	IP Spoofing atak koruma özelliği destekliyor mu?	1			BAŞARILI
GF_GD.2	Port taramalara karşı koruma sağlıyor mu?	1			BAŞARILI
GF_GD.3	TCP Protokolü 3'lü el sıkışma kontrolü sağlıyor mu?(Asimetrik rota ile test edilebilir.)	1			BAŞARILI
GF_GD.4	TCP Split Handshake atağına karşı önlem alabiliyor mu?	1			BAŞARILI
GF_GD.5	TCP Syn anormallik engelleme özelliğini destekliyor mu?(Syn paketinde veri taşınması)		1		BAŞARILI
GF_GD.6	Parçalanmış paket kontrolü ve engellenmesi özelliğini destekliyor mu?	1			BAŞARILI
GF_GD.7	Arabirimler arası erişim denetimi sağlıyor mu?	1			BAŞARILI
GF_GD.8	Kural aksiyonları olarak ACCEPT/DENY/LOG özelliklerini destekliyor mu?	1			BAŞARILI
GF_GD.9	Dos/Ddos engelleme özelliğini destekliyor mu? (ICMP Flood, UDP Flood, Connection Flood, SYN, ACK, FIN Flood)		1		BAŞARILI
GF_GD.10	Kullanıcı/Grup/Zaman bazlı güvenlik duvarı kuralı yazımını destekliyor mu?		1		BAŞARILI
GF_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?	1			BAŞARILI
GF_GD.12	IP-MAC eşleme destekliyor mu?	1			BAŞARILI
GF_GD.13	Kural derleme sırasında izni olmayan bir erişimin paket iletimini engelliyor mu?	1			BAŞARILI
GF_GD.14	Uygulama tanıma/engelleme özelliğini destekliyor mu? (Ör. Dosya transferi, Sanal özel Ağ ve tünel uygulamaları, Vekil sunucu uygulamaları, Uzaktan erişim uygulamaları)		1		BAŞARILI
GF_GD.15	Uygulama tanıma sırasında paket kaçırmamayı destekliyor mu?			1	BAŞARILI
GF_YT	Yetkilendirme Testleri				
GF_YT.1	Active Directory, LDAP yetkilendirme/entegrasyon yöntemlerini destekliyor mu?		1		BAŞARILI
GF_SED	SSH Erişimi Denetimi				
GF_SED.1	SSH üzerinden tünel erişimini engellemeyi destekliyor mu?			1	BAŞARILI

GF_SED.2	SSH üzerinde dosya paylaşımını engellemeyi destekliyor mu?			1	BAŞARILI
GF_STO	Saldırı Tespit ve Önleme (False/True Positive)				
GF_STO.1	Exploit saldırılarına karşı imza desteği var mı?		1		BAŞARILI
GF_STO.2	Phishing saldırılarına karşı imza desteği var mı?		1		BAŞARILI
GF_STO.3	Trojan/Malware saldırılarına karşı imza desteği var mı?		1		KISMEN BAŞARILI
GF_STO.4	Brute Force saldırılarına karşı imza desteği var mı?		1		BAŞARILI
GF_STO.5	Code/Command Execution saldırılarına karşı imza desteği var mı?		1		BAŞARILI
GF_STO.6	Tarayıcı odaklı saldırılara karşı imza desteği var mı?		1		BAŞARILI
GF_STO.7	Protokol anormallik tespiti desteği var mı?		1		BAŞARILI
GF_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)		1		BAŞARILI
GF_WF	Web Filtreleme (Http, Https)				
GF_WF.1	Kullanıcı/Grup/Zaman bazlı kural yazımını destekliyor mu?	1			BAŞARILI
GF_WF.2	URL, Alan adı, içerik, içerik tipi, eklenti, kelime, düzenli ifade(regex) engellemeyi destekliyor mu?	1			BAŞARILI
GF_WF.3	Kategori bazlı filtrelemeyi destekliyor mu?	1			BAŞARILI
GF_WF.4	Zayıf SSL algoritmalarını engelleme özelliğini destekliyor mu?			1	BAŞARILI
GF_WF.5	XFF(x-forwarded-for) kontrolü sağlıyor mu?		1		BAŞARILI
GF_AV	Anti-Virüs (http, https)				
GF_AV.1	Dosya uzantısına göre engelleme desteği var mı?	1			BAŞARILI
GF_AV.2	Eicar virüs dosyası ve içerik testi ile engelleme testini geçti mi?	1			BAŞARILI
GF_AV.3	Sıkıştırılmış dosya virüs testini geçti mi?	1			BAŞARILI
GF_AV.4	Ofis makro eklenti engelleme özelliğini destekliyor mu?	1			BAŞARILI
GF_AV.5	Wannacry için engelleme desteği sağlıyor mu?		1		KISMEN BAŞARILI
GF_AV.6	Malware/Trojan türü zararlıların engellenmesini destekliyor mu?		1		KISMEN BAŞARILI
GF_EG	Eposta Güvenliği				
GF_EG.1	Yetkilendirme olmadan eposta gönderen kullanıcının engellenmesini destekliyor mu?		1		BAŞARILI
GF_EG.2	Relay maillerin engellenmesini destekliyor mu?		1		BAŞARILI
GF_EG.3	E-posta seli saldırılarına karşı koruma/hafifletme desteği var mı?		1		BAŞARILI
GF_EG.4	Spam mail engellemeyi sağlıyor mu?		1		BAŞARILI

GF_EG.5	RBL Server desteği var mı?		1		BAŞARILI
GF_EG.6	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)			1	BAŞARILI
GF_EG.7	Üreticinin kendi tehdit güncelleme servisi ile desteklediği bir kara liste (blacklist) desteği var mı ?		1		BAŞARILI
GF_DNS	DNS (Alan adı sistemi)				
GF_DNS.1	DNS Sorgu tipine göre engelleme desteği var mı?			1	BAŞARILI
GF_DNS.2	Kara Liste ve Beyaz Listeler oluşturmayı destekliyor mu?			1	BAŞARILI
GF_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)			1	BAŞARILI
GF_YS	Yedeklilik Sistemi Testi				
GF_YS.1	Aktif-Pasif yedekli çalışmayı destekliyor mu?		1		BAŞARILI
	3- Temel Özellikler				
TO_SO	Sistem özellikleri				
TO_SO.1	Cihazın web veya masaüstü arabirimlerinden yönetilebiliyor mu?	1			BAŞARILI
TO_SO.2	SSH veya Seri Porttan Erişim Sağlanabiliyor mu ?	1			BAŞARILI
TO_SO.3	Disk yedekliliği açısından raid desteği var mı ?			1	BAŞARILI
TO_SO.4	Yönetim arabirimi Türkçe ve İngilizce olmak üzere en az iki dil desteğini sağlıyor mu?	1			BAŞARILI
TO_SO.5	Syslog ve SNMPv2,v3 desteği var mı?		1		BAŞARILI
TO_SO.6	Web giriş şifresini console'den resetleyebilme özelliği var mı?	1			BAŞARILI
TO_SO.7	Güncelleme desteği var mı ?	1			BAŞARILI
TO_SO.8	Konfig. bilgisini yedekleme ve geri dönme özelliği var mı?	1			BAŞARILI
TO_SO.9	Yedekli kurulumu destekliyor mu? (NAT, Router, Bridge modlarda)			1	BAŞARILI
TO_SO.10	IPv6 Ağ yapılandırma ve yönlendirme destekliyor mu?	1			BAŞARILI
TO_SO.11	IPv6 NAT64, 6to4, DualStackTunnel destekliyor mu?			1	BAŞARILI
TO_SO.12	Sistem, IPS, URL filtering v.b. tanımlarını "Offline (Internet'e bağlanmadan) güncelleme yapabiliyor mu?			1	BAŞARILI
TO_SO.13	Cihaz yöneticileri için Sertifika bazlı kimlik doğrulama yapabiliyor mu ?		1		BAŞARILI

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.)	1			BAŞARILI
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.)	1			BAŞARILI
TO_SO.16	SSL Inspection yapabiliyor mu ?	1			BAŞARILI
TO_KY	Kullanıcı yönetimi ve entegrasyon özellikleri				
TO_KY.1	Yerel kullanıcı ve grup eklenebiliyor mu?	1			BAŞARILI
TO_KY.2	Microsoft Active Directory NTLM veya Kerberos entegrasyonu destekleniyor mu?		1		BAŞARILI
TO_KY.3	Çoklu LDAP entegrasyonu desteği var mı?		1		BAŞARILI
TO_KY.4	Kullanıcılar için radius doğrulama servisi var mıdır ?		1		BAŞARILI
TO_KY.5	Güvenlik duvarında kullanıcı/grup kullanılabilir mi?		1		BAŞARILI
TO_KY.6	Uygulama kontrolünde kullanıcı/grup kullanılabilir mi?		1		BAŞARILI
TO_KY.7	Web filtrede kullanıcı/grup kullanılabilir mi?	1			BAŞARILI
TO_KY.8	Kullanıcı giriş portalında kullanıcı/grup kullanılabilir mi?	1			BAŞARILI
TO_KY.9	SSLVPN'de kullanıcı/grup kullanılabilir mi?		1		BAŞARILI
TO_KY.10	IDS-IPS gibi yerlerde kullanıcı/grup kullanılabilir mi?		1		BAŞARILI
TO_KY.11	Kullanıcı/Grup için kullanım zamanı ve veri indirme kotası ayarlanabilir mi?		1		BAŞARILI
TO_AO	Ağ özellikleri				
TO_AO.1	10/100/1000 fiziksel arabirim ve PPPOE, VLAN, BRIDGE, LACP(BOND), LOOPBACK yazılımsal arabirim desteği var mı?	1			BAŞARILI
TO_AO.2	10 Gigabit fiziksel arabirim desteği var mı?			1	BAŞARILI
TO_AO.3	3G/4G Internet aygıtları yazılımsal arabirim desteği var mı?		1		BAŞARILI
TO_AO.4	Tek noktaya (Unicast), Çok noktaya (Multicast) yönlendirme özellikleri var mı?		1		BAŞARILI
TO_AO.5	Politika tabanlı ve dinamik(bgp, ospf vs.) yönlendirme özellikleri var mı?		1		BAŞARILI
TO_AO.6	NAT, Router mod desteği var mı?	1			BAŞARILI
TO_AO.7	Bridge mod desteği var mı?		1		BAŞARILI
TO_AO.8	LLDP(Link Layer Discovery Protocol) özelliği var mı?			1	BAŞARILI
TO_AO.9	DHCP servisi var mıdır ve her arabirimi özelleştirebiliyor mu?	1			BAŞARILI
TO_AO.10	DNS önbellek servisi var mı ?	1			BAŞARILI
TO_AO.11	Çoklu internet hattı desteği var mı?	1			BAŞARILI

TO_AO.12	Kural tabanlı internet yük dengeleme ve hata kontrolü desteği ile otomatik internet hattı değişimi yapabiliyor mu?		1	BAŞARILI
TO_AO.13	Farklı tip hatları (xDSL, 3G/4.5G, ME) birleştirme yapabiliyor mu?		1	BAŞARILI
TO_AO.14	Her bir ethernet portu özelleştirilebiliyor mu?	1		BAŞARILI
TO_SAO	Sanal özel ağ özellikleri			
TO_SAO.1	Güvenli bağlantı için VPN (L2TP over IPSec, SSLVPN) desteği var mı?	1		BAŞARILI
TO_SAO.2	Noktadan-Noktaya IPSec VPN (IKEv1-v2) desteği var mı?	1		BAŞARILI
TO_SAO.3	IPSec, SSLVPN ve L2TP over IPSec VPN türleri en az AES şifreleme yöntemlerini ve SHA doğrulama yöntemlerini destekliyor mu?	1		BAŞARILI
TO_GD	Güvenlik duvarı özellikleri	1		
TO_GD.1	Kural yazılırken oturum kontrollü/kontROLSÜZ yazılabiliyor mu ?	1		BAŞARILI
TO_GD.2	Parçalanmış paket kontrolü ve engellemesi var mı?	1		BAŞARILI
TO_GD.3	IP, ağ adresi, IP aralığı gibi nesneler kullanılarak kural yazılabiliyor mu?	1		BAŞARILI
TO_GD.4	Kullanıcı/Grup kullanılarak kural yazılabiliyor mu?		1	BAŞARILI
TO_GD.5	Kural aksiyonu olarak izin ver/engelle/kayıt(log) seçeneklerini barındırıyor mu?	1		BAŞARILI
TO_GD.6	NAT-PAT destekleniyor mu?	1		BAŞARILI
TO_GD.7	IP-MAC eşleştirme destekleniyor mu?	1		BAŞARILI
TO_GD.8	L7 Uygulama tanımlı kural yazımını destekliyor mu?		1	BAŞARILI
TO_GD.9	SSL protokolü ile çalışan uygulamaları da tanıyıp aksiyon alabiliyor mu?		1	BAŞARILI
TO_GD.10	IP spoofing saldırı koruma özelliği var mıdır ?	1		BAŞARILI
TO_GD.11	TCP SYN paketlerindeki anormallik tespiti yapabiliyor mu ?		1	BAŞARILI
TO_GD.12	Temel DoS/DDoS koruması(minimum SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood, Connection Flood) sağlıyor mu?		1	BAŞARILI
TO_GD.13	DDoS korumaya(minimum SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood, Connection Flood) özel politika bazlı kural yazabilmeye imkan tanıyor mu?		1	BAŞARILI
TO_GD.14	Zaman tanımlı kural yazımını destekliyor mu?	1		BAŞARILI
TO_GD.15	Dışarıdan tespit edilmemesi için management portlar kapatılabiliyor mu ?	1		BAŞARILI
TO_GD.16	Politika bazlı yönlendirme desteği var mıdır?	1		BAŞARILI
TO_GD.17	DHCP servisinde tanımlanan MAC-IP adreslerinin dışında IP almasını engellenebiliyor mu?	1		BAŞARILI
TO_GD.18	Port, uygulama ve IP bazında QoS servisi destekliyor mu ?		1	BAŞARILI
TO_SSH	SSH derin inceleme özellikleri			

Ankara Teknopark
İvedik OSB Mahallesi 2224.Cadde 1/250 C Blok Kat:13
Yenimahalle /ANKARA

TRTEST                                         

TO_KGP	Kullanıcı giriş portalı (Hotspot/Captive Portal) özellikleri				
TO_KGP.1	Hotspot bağlantı için SMS ile doğrulama yapabiliyor mu?		1		BAŞARILI
TO_KGP.2	Hotspot bağlantı için Özel SMS API bağlantısı ile doğrulama yapabiliyor mu?		1		BAŞARILI
TO_KGP.3	Hotspot bağlantı için T.C. Kimlik ile doğrulama yapabiliyor mu?		1		BAŞARILI
TO_KGP.4	Hotspot bağlantı için LDAP ile doğrulama yapabiliyor mu?		1		BAŞARILI
TO_KGP.5	Hotspot bağlantı için Lokal kullanıcı ile doğrulama yapabiliyor mu?	1			BAŞARILI
TO_KGP.6	Hotspot bağlantı için 3'üncü parti veri tabanları ile doğrulama yapabiliyor mu?			1	BAŞARILI
TO_KGP.7	Hotspot da farklı dil desteği var mı ve farklı profil oluşturulabiliyor mu ?	1			BAŞARILI
TO_KGP.8	Kullanıcılarına zaman ve veri kotası uygulanabiliyor mu ?		1		BAŞARILI
TO_KGP.9	Müşteriye göre hotspot ekranı özelleştirilebiliyor mu ?		1		BAŞARILI
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) mühürlenebiliyor mu ?	1			BAŞARILI
TO_KG.2	Log kayıtlarında kullanıcı bilgisi, kaynak-hedef IP bilgisi değerleri var mı?	1			BAŞARILI
TO_KG.3	Log kayıtlarında uygulama adı ve kural numarası gibi değerler var mı?		1		BAŞARILI
TO_KG.4	Oturum başlangıç-bitiş zamanları, paket ve veri miktarı ile ilgili kayıtlar tutuluyor mu?			1	BAŞARILI
TO_KG.5	İmzalanmış log kayıtlarını yasal zorunluluk olan en az 2 yıl saklayabiliyor mu ?	1			BAŞARILI
TO_KG.6	Log kayıtları lokal diskin dışında uzak sistemlere gönderilebiliyor mu (ftp, scp, smb, syslog)?		1		BAŞARILI
TO_KG.7	Oluşan log kayıtları canlı incelenebiliyor mu?	1			BAŞARILI
TO_KG.8	Oluşan log kayıtları geriye doğru incelenebiliyor mu?		1		BAŞARILI
TO_R	Raporlama özellikleri				
TO_R.1	Default şablonlar ile hızlı rapor alınabiliyor mu ?	1			BAŞARILI
TO_R.2	Raporların çıktısını özelleştirebiliyor muyuz ?		1		BAŞARILI
TO_R.3	Yönetim, Güvenlik duvarı, web filtre, DHCP, hot spot, oturum geçmiş, anti-virüs/anti-spam, IPS kayıtları ile ilgili raporlar alınabiliyor mu?		1		BAŞARILI

TO_I	İzleme özellikleri			
TO_I.1	Dashboard ekranı üzerinde görsel özelleştirme yapılabiliyor mu?		1	BAŞARILI
TO_I.2	Dashboard ekranında veya monitoring yazılımlarında ağ trafiği canlı ve grafiksel izlenebiliyor mu?	1		BAŞARILI
TO_I.3	IPSec, SSLVPN, Hot spot gibi modüllerin bağlı kullanıcılarının bağlantı durumları izlenebiliyor mu?	1		BAŞARILI
TO_I.4	Dashboard ekranında donanım kaynakları izlenebiliyor mu?	1		BAŞARILI
TO_UD	Ürün dokümantasyonu			
TO_UD.1	Türkçe ve İngilizce doküman desteği var mıdır?	1		BAŞARILI
TO_UD.2	Ürün kutusu içerisinde hızlı kurulum, ürün özellikleri ve saklama koşullarını gösteren yazılı veya elektronik yönetici el kitabı yer alıyor mu?	1		BAŞARILI
TO_UD.3	Üreticinin ürüne ilişkin forum/bilgi deposu ve çağrı sistemi web sayfaları var mı?	1		BAŞARILI
TO_UD.4	Üretici web sayfasında sık sorulan sorular veya ürünle alakalı makale, blog sayfası var mıdır?		1	BAŞARILI
TO_UD.5	Youtube veya benzeri video paylaşım sitelerinde ürünün temel özellikleri ile ilgili kurulum veya yapılandırma videoları var mıdır?			1 BAŞARILI
TO_UD.6	Ürünün üretici tarafından yayınlanan güncellemelerine ilişkin sürüm notları ile ilgili doküman müşteriler tarafından çevrimiçi erişilebiliyor mu?		1	BAŞARILI
	4. Performans / Kapasite			
PK.1	Ürün üretici tarafından beyan edilen performans kriterlerini sağlıyor mu?	1		BAŞARILI
PK.2	Üretici tarafından test ortamı ve test edilecek ürünün modeli belirtilmiş mi?	1		BAŞARILI
PK.3	Ürüne ilişkin aşağıdaki testler (sarı renli testler zorunlu) yapılarak performans raporu alınmalıdır.			
Maksimum Kapasite	Maksimum Eşzamanlı Teorik TCP Bağlantısı			BAŞARILI
	Saniyedeki maksimum Yeni TCP Bağlantısı			BAŞARILI
	Saniyedeki maksimum HTTP Bağlantısı			BAŞARILI
	Saniyedeki maksimum HTTP Hareketi (ing: transaction)			BAŞARILI
	Maksimum eşzamanlı IPSec bağlantısı.			BAŞARILI
	Maksimum eşzamanlı SSLVPN bağlantısı			BAŞARILI
Sistem Çıktısı (Throughput) Performansı	• Farklı Çerçeve Boylarında (1518 byte, 512 byte, 64 byte traffic, IMIX) Güvenlik Duvarı (Mbps olarak başarı ile taşınabilen maksimum hızın(ing: rate) ölçülmesi amaçlanır.)			
	• Güvenlik Duvarı ve HTTP Proxy olarak (antivirüs ile birlikte ve antivirüs olmadan)			BAŞARILI
	• Güvenlik Duvarı ve HTTPS olarak			BAŞARILI

	Güvenlik Duvarı ve IPS olarak			BAŞARILI
	Güvenlik Duvarı, HTTP ve IPS olarak			BAŞARILI
	UTM, Next Generation (eğer uygulanabilirse)			BAŞARILI
	IPSec site-to-site throughput test			BAŞARILI
Ham Paket İşleme Performansı (UDP Throughput)	64 Byte Paketler			BAŞARILI
	128 Byte Paketler			BAŞARILI
	256 Byte Paketler			BAŞARILI
	512 Byte Paketler			BAŞARILI
	1024 Byte Paketler			BAŞARILI
	1514 Byte Paketler			BAŞARILI
	Jumbo Paketler			BAŞARILI
Gecikme (Latency)	64 Byte Çerçeveler			BAŞARILI
	128 Byte Çerçeveler			BAŞARILI
	256 Byte Paketler			BAŞARILI
	512 Byte Paketler			BAŞARILI
	1024 Byte Paketler			BAŞARILI
	1514 Byte Paketler			BAŞARILI
	Jumbo Paketler			BAŞARILI
SSL/TLS Performansı	HTTPS Filtreleme Performansı			BAŞARILI
Karışık Trafik	Bütün UTM fonksiyonlarının aynı anda açık olduğu durumda ve karışık trafik üretilerek performans testi yapılabilir. (Güvenlik Duvarı, NGFW) o %70 HTTPS and %30 HTTP			BAŞARILI
	Özel sektör dikeylerini ve / veya kullanım durumlarını temsil eden trafik karışımları geliştirilmelidir.			BAŞARILI
Esneklik (Resiliency)	Yüksek Erişilebilirlik High Availability (Varsa belirtilmelidir)			BAŞARILI
	By Pass Desteği (Varsa Belirtilmelidir.)			BAŞARILI
PK_GDP	Güvenlik duvarının performansı			
PK_GDP.1	Güvenlik Duvarı, trafiği ayrıştırma seviyesine göre öncelik sırasına koyabiliyor mu?	1		BAŞARILI
PK_GDP.2	Garantili bant genişliği ile VOIP ve Video konferans trafiğini önceliklendirebiliyor mu?	1		BAŞARILI
PK_GDP.3	Güvenlik duvarı, performans istatistiklerini, paket kayıplarını, sistem kaynakları kullanımını gösteriyor mu?	1		BAŞARILI
	5- REGÜLASYONLARA UYUM			
RU_TCK	TCK 5651/5070	1		
RU_TCK.1	Kanunun kayıt tutma hükümlerine uyumluluğu var mı?	1		BAŞARILI
RU_TCK.2	Kanunun zaman damgası kriterlerine göre 5070 sayılı kanun tarafından yetkilendirilmiş bir zaman damgası kullanımını destekliyor mu?	1		BAŞARILI

RU_TCK.3	Kanunun katalog suçların engellenmesi hükümlerine uyumluluğu var mı?	1		BAŞARILI
RU_TCK.4	Kanunun refere ettiği yönetmelik ve benzeri mevzuat ile uyumluluğu var mı?	1		BAŞARILI
RU_KVKK	KVKK	1		
RU_KVKK.1	Ürün hotspot kullanımı sırasında Kişisel Verilerin Kullanımı ile ilgili sözleşme bilgilendirme ve onay alma sistemini destekliyor mu?	1		BAŞARILI
RU_KVKK.2	Ürün kişisel verileri, sözleşme ve bilgilendirmelere aykırı şekilde, cihaz dışına transfer etmediğini onaylıyor mu?		1	BAŞARILI
RU_KVKK.3	Ürün kişisel verileri cihaz dışına transfer ediyorsa buna baz olacak kişisel verilerin kullanımı sözleşmesi bilgilendirme ve onayını aldığını kanıtlatabiliyor mu?	1		BAŞARILI

2 Test Durumu:

EPATİ BİLİŞİM TEKNOLOJİLERİ SAN. VE TİC. LTD. ŞTİ. firmasının ANTİKOR v2.0 ürün grubuna yönelik yapılan testlere ilişkin test durumu bilgisi aşağıda yer almaktadır.

	C	B	A	Toplam
1 Ürün Güvenliği				
1.1 Web Arayüzleri Zayıflık taraması	10	4		14
1.2 Konsol				
1.2.a Seri Port/Monitor	4			4
1.2.b Ağ Üzerinden Erişim (SSH/Telnet Vb)	7			7
1.3. Diğer (Uygulama/API/Mobil varsa Yönetim)	8	2		10
İşletim Sistemi ve Servisler	5	1	2	8
Masumiyet Testi	2			2
2 Güvenlik Fonksiyon Testi				
Güvenlik Duvarı	10	4	1	15
Yetkilendirme Testleri		1		1
SSH Erişim Denetimi			2	2
Saldırı Tespit Ve Önleme (False/True Positive)		8		8
Web Filtreleme (Http, Https)	3	1	1	5
Anti-Virüs (http, https)	4	2		6
E-posta Güvenliği		6	1	7
DNS (Alan adı sistemi)			3	3
Yedeklilik Sistemi Testi			1	1
3 Temel Özellikler				
Sistem Özellikleri	10	3	3	16

Ankara Teknopark
 İvedik OSB Mahallesi 2224.Cadde 1/250 C Blok Kat:13
 Yenimahalle /ANKARA

Bilgi için: Büşra Nur YÜZER,
 Telefon No:0 850 551 00 00 /25

TRTEST       iştirakidir.

TRTEST TEST VE DEĞERLENDİRME A.Ş.
 İvedik O.S.B. Mahallesi 2224. Cadde No:1 / 250
 Yenimahalle / ANKARA
 Ulus V.D. 859 064 7 995 Tic.Sic.No:415473
 Mersis No: 0859 0647 9950 0001

Kullanıcı yönetimi ve entegrasyon özellikleri	3	8		11
Ağ özellikleri	6	6	2	14
Sanal özel ağ özellikleri	3			3
Güvenlik duvarı özellikleri	11	6	1	18
SSH derin inceleme özellikleri			2	2
Web filtre özellikleri	8			8
DNS filtreleme özellikleri			2	2
Saldırı tespit ve önleme özellikleri		4	1	5
E-Posta güvenliği özellikleri		5		5
Kullanıcı giriş portalı (Hotspot/Captive Portal) özellikleri	2	6	1	9
Kayıt altına alma ve görüntüleme özellikleri	4	3	1	8
Raporlama Özellikleri	1	2		3
İzleme Özellikleri	3	1		4
Ürün dokümantasyonu	3	2	1	6
4 Kapasite/performans	2			2
Performans	31			31
Güvenlik duvarının performansı		3		3
5 Regülasyonlara Uyum				
TCK 5651/5070	4			4
KVKK	2	1		3
		Genel Toplam		250

DURUM	A	B	C	P	Toplam
BAŞARILI	24	77	115	31	250
KISMEN BAŞARILI	-	3	-	-	250

- Toplamda 250 madde test edilmiş ve test maddesine ilişkin “BAŞARILI” ya da “BAŞARISIZ” durumu 1.3 Özet Test Sonuçları tablosunda belirtilmiştir.
- Testleri tamamlanan FIREWALL ürün grubunda EPATİ BİLİŞİM TEKNOLOJİLERİ SAN. VE TİC. LTD. ŞTİ. Firması Antikor ürünü testlerinde herhangi bir zafiyet bulunmamış olup, bu kapsamda yapılan testlerden başarı ile geçtiklerinden dolayı yapılan inceleme ve değerlendirme neticesinde TRTEST tarafından Ürün Uygunluk Sertifikası almaya hak kazanmıştır.