FMV IŞIK ÜNİVERSİTESİ

3 YILLIK
GÜVENLIK DUVARI ALIMI

1 Güvenlik duvarı (2 Adet)

1.1 Genel

1.1.1 Güvenlik duvarı ürünleri özel üretilmiş bir donanım ve yazılım bütünü cihaz (appliance) olarak teklif edilecektir.

1.1.2 Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, "NSS Labs Next Generation Firewall (NGFW)" testlerine girmiş olması gereklidir.

1.1.3 Güvenlik duvarı üreticisi "2017, 2018, 2019 ve 2020 Gartner Magic Quadrant for Enterprise Network Firewalls" raporunda "Leaders" kategorisinde yer almalıdır.

1.1.4 Güvenlik duvarı üzerinde Firewall, VPN, IPS, Uygulama Kontrolü, İçerik(URL) Filtreleme, Anti Virüs ve Anti Bot güvenlik bileşenleri çalıştırılacaktır.

1.1.5 Teklif edilecek 2 adet güvenlik duvarı ürünü istenen güvenlik bileşenleri aynı anda devredeyken cluster mimarisinde yedekli çalışmayı destekleyecektir. Bu amaçla cihazlar üzerinde ayrı bir bağlantı portu gerekiyorsa bu sağlanacaktır.

1.1.6 Güvenlik duvarı Threat Prevention fonksiyonları (Firewall, Uygulama Kontrolü, URL Filtreleme, IPS, Anti-Virüs, Anti-Bot ve Sıfırıncı Gün) devredeyken enterprise test ortamında en az 2.5 Gbps throughput kapasitesine

sahip olacaktır. Bu değerler teklif edilen ürün ile ilgili dokümanlarda belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

1.1.7 Güvenlik duvarı en az 2.000.000 adet eş zamanlı oturumu (concurrent connections) desteklemelidir.

1.1.8 Güvenlik duvarı en az 90.000 adet anlık bağlantı isteğini (connections per second) karşılayabilmelidir.

1.1.9 Güvenlik duvarı üzerinde en az 240GB kapasiteli SSD disk bulunmalıdır.

1.1.10 Güvenlik duvarı üzerinde en az 10 adet 10/100/1000 Mbps bakır ethernet port bulunmalıdır.

1.1.11 Güvenlik duvarı üretici firma tarafından geliştirilmiş ve güçlendirilmiş özel bir işletim sistemi üzerinde çalışacaktır.

1.1.12 Mimari açıdan stateful inspection ve IP paket filtreleme özelliklerini bünyesinde bulundurmalıdır.

1.1.13 En az 1024 adet VLAN desteklemelidir.

1.1.14 MS Active Directory ile entegre olarak kişi, grup bazında firewall kuralı yazılmasına, tutulan kayıtlarda kullanıcı isminin görülmesine olanak sağlayabilmelidir.

1.1.15 Ülke/kıta bazında tüm IP adreslerini kapsayacak ya da Google/Amazon/Office365 gibi bulut servisleri için IP adresi yazmaya gerek kalmadan kural yazılabilmelidir. Buradaki IP adresleri dinamik olarak güncellenecek, elle manuel mudaheleye gerek kalmayacaktır.

1.1.16 OSI Layer-3 ile Layer-7 arasındaki ağ trafiğini izleyebilmelidir.

1.1.17 İnternette kullanılan her servisi; TCP, UDP, RPC ve ICMP tabanlı protokolleri desteklemelidir. Kullanıcı tanımlı servis hizmeti tanımlamaya izin vermelidir.

1.1.18 Saat, gün, tarih, periyot bazında erişim kontrolü yapabilmelidir.

1.1.19 Yerel ağdaki bir ya da birden fazla adres aralığındaki birçok IP'yi istenirse tek bir adres arkasında, istenirse her bir aralığı başka bir tek adres arkasında saklayabilmeli ya da bire bir adres çevrim özelliği (NAT) olmalıdır.

1.1.20 Port adres çevrim (PAT) özelliğine sahip olmalıdır.

1.1.21 Bant genişliği kontrolü (QoS) yapabilmelidir. Bu özellik ile kaynak/hedef veya servis bazında bant genişliği kullanımını limitleyebilmeli, garanti edebilmelidir.

1.1.22 Static Route, kaynak tabanlı yönlendirme, (Politika tabanlı Yönlendirme) RIP, OSPF, BGP gibi dinamik yönlendirme protokollerini desteklemeli ve bu özellikler ile teklif edilmelidir.

1.1.23 IPv6 desteği olmalıdır.

1.1.24 Cihaz üzerinde yedekli olacak şekilde 2 adet güç kaynağı (power supply) bulunacaktır.

1.2 IPSEC VPN

1.2.1 Güvenlik duvarının VPN yapabilme özelliği olmalıdır.

1.2.2 IPSec VPN standardını desteklemeli, Site to Site ve Client to Site VPN bağlantı yapabilmelidir.

1.3 IPS

1.3.1 Güvenlik duvarının IPS özelliği olmalıdır.

1.3.2 Farklı ülkelerden gelebilecek trafiği tehdit/saldırı anında kesebilmelidir. Coğrafi koruma sağlayabilmelidir.

1.3.3 IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza icin ayrı ayrı ayarlanabilmelidir.

1.3.4 IPS özelliğinde saldırılara karşı kullanılan filtreler, güncelleme dosyasından ya da internet üzerinden güncellenebilmelidir. Ayrıca eğer istenirse, imza güncellemeleri kullanıcı müdahalesi olmadan otomatik olarak da yapılabilmelidir.

1.3.5 IPS fonksiyonu aşağıdaki saldırı tiplerine karşı koyabilmelidir;

- Backdoors
- Botnets
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Anlık mesajlaşma (Skype, vb.)
- İşletim sistemlerine dönük saldırılar
- Peer-to-peer (BitTorrent, Ares, vb.)
- Protocol tunneling
- Traffic Anomaly
- Protocol Anomaly

1.4 Uygulama Kontrolü

1.4.1 Güvenlik duvarının uygulama kontrolü özelliği olmalıdır.

1.4.2 En az 8.000 adet uygulamayı tanıyabilmelidir.

1.4.3 En az 260.000 adet sosyal ağ widget (social network widget) tanıyabilmelidir.

1.4.4 Uygulama kontrolü özelliği active directory ile entegre çalışabilecek bu sayede MS Active Directory'de tanımlı olan kullanıcı ve gruplar bazında uygulama kontrolü kuralları tanımlanabilmelidir.

1.4.5 Uygulama bloklama ve uyarı portalı özelleştirilebilir olmalı ve Türkçe desteği bulunmalıdır.

1.4.6 Tüm uygulamalar için farklı bantgenişliği sınırlamaları tanımlanabilmelidir.

1.5 URL Filtreleme

1.5.1 Güvenlik duvarının URL filtreleme özelliği olmalıdır.

1.5.2 En az 200 milyon URL adresine sahip bir veritabanı olmalı, bu URL adresler en az 60 kategoride gruplanmış olmalıdır.

1.5.3 URL filtreleme özelliği, MS Active Directory ile entegre çalışabilecek bu sayede MS Active Directory'de tanımlı olan kullanıcı ve gruplar bazında URL filtreleme kuralları tanımlanabilecektir.

1.5.4 Tüm URL veya URL kategorileri için farklı bant genişliği sınırlamaları tanımlanabilmelidir.

1.5.5 URL bloklama ve uyarı portalı özelleştirilebilir olmalı ve Türkçe desteği bulunmalıdır.

1.6 Anti Virüs

1.6.1 Güvenlik duvarının Anti Virüs özelliği olmalıdır.

1.6.2 SMTP, HTTP/HTTPS ve FTP trafiğini virüse karşı tarayabilmeli, tarama işlemini her protokol için trafiğin yönüne ve kaynak/hedef adrese göre yapabilmelidir.

1.6.3 Bilinen virüsler için imza temelli bloklama yapabilmelidir.

1.6.4 Anti Virüs mimarisi MS Active Directory ile entegre çalışabilecek bu sayede MS Active Directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında Anti Virüs kuralları tanımlanabilecektir.

1.7 Anti Bot

1.7.1 Cihaz üzerinde detayları aşağıda iletilen botnet tespit ve engelleme özelliği olmalıdır.

1.7.2 Port ve protokolden bağımsız çalışmalı, internete doğru yapılan tüm ip trafiğini inceleyebilmelidir.

1.7.3 Botnet komuta kontrol merkezlerine erişim için yapılan adres çözümleme isteklerini tespit ve dns sorgusu esnasında trafiği bloklayabilme özelliğine sahip olmalıdır.

1.7.4 Bilinmeyen komuta kontrol merkezleriyle yapılan iletişimler için davranışsal analiz yapabilmeli bu sayede şüpheli trafiği engelleyebilmelidir.

1.7.5 Bilinen botnet'ler için imza temelli bloklama yapabilmelidir. Her bir botnet imzası için alınabilecek aksiyonlar sistem yöneticileri tarafından konfigüre edilebilmelidir.

1.7.6 Farklı kullanıcı veya kullanıcı grupları için farklı botnet politikaları oluşturulabilmelidir.

1.7.7 Botnet tespit ve engelleme mimarisi active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında botnet filtreleme kuralları tanımlanabilecektir.

1.8 HTTPS Inspection

1.8.1 Güvenlik duvarı HTTPS trafiğini inceleyerek, IPS, Uygulama Kontrolü, URL Filtreleme ve Anti Virüs kontrollerini uygulayabilmelidir.

1.8.2 Inbound (giriş) yönünde HTTPS inspection yaparak, kurum içindeki bilgisayar ve sunucuları internetten gelecek olası saldırılara karşı koruyabilmeli, Outbound (çıkış) yönünde HTTPS inspection yaparak, kurum içindeki bilgisayar ve sunuculardan başka bir kuruma yapılabilecek olası saldırıları engelleyebilmelidir.

1.8.3 HTTPS trafiğinin incelenmesi için erişim rolü, bilgisayar/sunucu, ağ bazında kural yazılabilmelidir.

1.8.4 HTTPS trafik içeriğinin görülmemesi istenen durumlar için (Bankacılık işlemleri, vb.) bypass (atlatma) kuralı yazılabilmelidir.

1.9 Yenileme / Destek Süresi

1.9.1 Teklif edilecek güvenlik duvarı ürünleri için 3 yıl süreyle yazılım güncellemesi, servis güncellemesi ve donanım garantisi sağlanmalıdır. Servis güncellemesi IPS, Uygulama Kontrolü, URL Filtreleme, Anti Virüs ve Anti Bot servislerini içermelidir.

2 Yönetim, Log Tutma ve Raporlama Sistemi – 1 Adet

Yönetim, log tutma ve raporlama sistemi bütünleşik olacaktır.

2.1 Yönetim ve Log Tutma Sistemi

2.1.1 Yönetim, log tutma ve raporlama sistemi yazılım olarak sağlanarak kurumda mevcut olan sanal platform (Vmware veya HyperV) üzerinde çalıştırılacaktır.

2.1.2 Yönetim, log tutma ve raporlama sistemi güvenlik duvarı ürünleri ile aynı üreticiye ait olmalıdır.

2.1.3 Sistem en az 2 adet güvenlik duvarı için gerekli lisansa sahip olmalıdır.

2.1.4 Önerilen sistem grafik arayüzden (GUI) yönetilecektir.

2.1.5 Yönetim sistemi sayesinde birden fazla güvenlik cihazı merkezi olarak tek bir arayüzden yönetilebilecektir.

2.1.6 Yönetim sistemi sayesinde, güvenlik cihazlarının kaynak kullanımları ve üzerinden geçen trafik miktarı gerçek zamanlı olarak görülebilecektir.

2.1.7 Güvenlik duvarı loglarını merkezi bir log tutma sistemine gönderecektir.

2.1.8 Güvenlik duvarı ile merkezi yönetim sistemi arasında bağlantı sorunu yaşanırsa, loglar tekrar iletişim kurulana kadar güvenlik duvarı üzerinde tutulacaktır.

2.1.9 Log tutma sistemi sayesinde loglar grafiksel olarak görülebilecek ve istendiğinde logun detayları görülebilecektir.

2.1.10 Log kayıtlarını ftp veya benzer bir protokolle harici bir sunucu veya depolama alanı üzerine arşivleyerek log yedekliliği sağlayabilmelidir.

2.2 Raporlama Sistemi

2.2.1 Önceden tanımlanmış rapor üretebilmelidir. Sistem kullanıcı tarafından tanımlanabilen özel raporları da üretebilmelidir.

2.2.2 Merkezi log tutma sistemi sayesinde loglar analiz edilebilecek ve raporlar üretilebilecektir.

2.2.3 Html, pdfveya benzer doküman formatlarında rapor üretebilmeli, üretilen raporları belirtilen e-mail adreslerine gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.

2.3 Uyumluluk (Compliance)

2.3.1 Önerilen güvenlik duvarı yönetim sistemi 1 yıl süreyle güvenlik politikası kurallarını bilinen uluslararası standartlarla (ISO 27001, ISO 27002, COBIT vb.) uyumluluğunu kontrol edebilecektir.

2.4 Yenileme / Destek Süresi

2.4.1 Yönetim, log tutma ve raporlama sistemi için 3 yıl süreyle yazılım güncellemesi sağlanmalıdır. Eğer çözüm donanım olarak teklif ediliyorsa 3 yıl süreyle donanım garantisi de sağlanmalıdır.

2.5 Güvenlik Duvarı Yazılım ve Donanım Yenilemesi

2.5.1 Kurumumuzu internetten gelecek tehditlere karşı koruyan GÜVENLİK DUVARI Yazılımının ve Donanımının Güncellemelerinin temin edilmesi gereklidir.

2.5.2 Aşağıda ki tabloda belirtilen, teklif edilecek Güvenlik Duvarı Donanım ve yazılım bileşenleri en az 3 yıllık Checkpoint Collobrative Standart(CPCES-CO-STANDARD-ADD) desteğini içermelidir.

Ürün Kodu	Açıklama
CPAP-SG5100-NGTP	5100 Next Generation Threat Prevention Appliance
CPAP-SG5100-NGTP-HA	5100 Next Generation Threat Prevention Appliance for High Availability
CPSM-NGSM5	Next Generation Security Management Software for 5 gateways (SmartEvent and Compliance 1 year)

2.5.3 Teklif edilecek Güvenlik Duvarı Donanımları için aşağıda bulunan ürünlerin servis güncellemeleri en az 3 yıllık olarak yapılmalıdır.

Servis Ürün Kodu	Servis Açıklama
CPAP-SG5100-NGTP	Enterprise Based Protection - Next Generation Threat Prevention Package Including IPS, APCL, URLF, AV, ABOT and ASPM blades
CPSM-NGSM5	SmartEvent and SmartReporter blade for 5 gateways (Smart-1 and open server) 3 year subscription