TEKNİK ŞARTNAME

İşin çeşidi : Merkezi Güvenlik Sistemi Donanım-Lisans Güncelleme

İşin niteliği : Mevcuttaki Palo Alto Merkezi Güvenlik Sistemi donanım ve lisans güncellemesi

Alınması planlanan ürünler:

2 adet PA-3420 ürününün PA-5410 model ile güncellemesi. Ürünlerle ilgili lisans ve garanti bakım hizmeti – 3 yıl
Palo Alto Panorama Yönetim Yazılımı lisans güncelleme hizmeti (PAN-PRA-25,PAN-SVC-BKLN-PRA-25 devices) – 3 yıl

Şartnamede;

İstanbul Bilgi Üniversitesi – BİLGİ, ,
Bilişim Teknolojileri Departmanı – BT Dept.
Teklif veren kuruluş, (FİRMA),
Satın alınması yapılacak donanım/yazılım/hizmet ÜRÜN
olarak anılacaktır.

ÖN KOŞULLAR

- İşbu şartname, BİLGİ'nin kendi lokasyonunda konuşlandırdığı PaloAlto Güvenlik Duvarı Donanım ve Yazılımlarının Güncellenmesi ile Panorama Yönetim Yazılımının lisansının güncellenmesi, artan kapasite ihtiyacının karşılanması için ihale kapsamındaki ÜRÜN'lerle ilgili alımın/hizmetin konusunda bilgi birikimine sahip olan FİRMA' dan yapılmasını kapsamaktadır.

- ÜRÜN teslim yeri, BİLGİ'nin Santral Kampusu – BT Dept.dır. ÜRÜN; üzerinde adı, tipi, modeli, seri numaraları ve üretici firma adını taşıyan orijinal ambalajlarda teslim edilecektir.

- FİRMA'nın teslim edeceği ÜRÜN fiyatları, BİLGİ'nin göstereceği adrese teslim fiyatlarıdır. Her türlü nakliye, navlun, sigorta, gümrük ve benzeri maliyetler dâhil fiyatlardır ve FİRMA tarafından karşılanacaktır. FİRMA, resmi teklifinde belirtmiş olduğu ÜRÜN fiyatları haricinde başka hiçbir koşul veya isim altında bedel talep etmeyecektir.

- ÜRÜN teslim süresi, sipariş tarihinden itibaren en fazla 6 haftadır. Ancak kanunlarda belirtilen mücbir sebeplerden dolayı teslim süresinin uzaması durumunda taraflar yeni teslim tarihi belirleyecektir. Mücbir sebep halleri dışındaki gecikmeler, cezaya tabidir.

- ÜRÜN' le birlikte sağlanan lisanslar BİLGİ adına kayıtlı ve son sürüm olmalı veya son sürüm FİRMA tarafından en geç teslimattan sonraki 2(iki) hafta içinde BT Dept. onayıyla yüklenmelidir.

- ÜRÜN' ün belirtilen sürede teslim edilmemesi veya teklif edilen ve onaylanan ÜRÜN' den farklı model/nitelikte getirilmesi durumunda, oluşacak zarardan dolayı BİLGİ'nin uğrayacağı maddi ve manevi tazminatlar FİRMA tarafından kayıtsız şartsız kabul edilecektir.

GENEL İSTEK VE ÖZELLİKLER

- Satın alınacak donanım ve yan donanımlar, FİRMA tarafından KURUM' un belirleyeceği yazılımlar (driver vb.) yüklenmiş ve çalışır vaziyette teslim edilmelidir.
- Satın alınacak her bir mal ve hizmete ait orijinal belge ve döküman (İngilizce ve/veya Türkçe) tam olarak kullanıcıya teslim edilecektir.
- ÜRÜN' ü oluşturan tüm parçalar yeni ve hiç kullanılmamış olmalı, ÜRÜN' ün en az 1 yıl aynı seride üretimi devam etmelidir. Aksi taktirde KURUM' un onaylayacağı bir üst model ürün sağlanmalıdır.
- Parçaların hiç bir bölümünde kırık, çatlak ve deformasyon hataları bulunmamalıdır.
- Satın alınacak donanımlar, uyumluluk ve yönetim kolaylığı nedeniyle için aynı markanın ürünü olmalıdır.
- Sistemlerin çalışması için gerekli her türlü bağlantı kablosu, güç kablosu, soket, konnektör ve buna benzer çeşitli donanımlar ve yazılımlar firma tarafından sağlanacaktır.
- Tüm sistem ve bağlı donanımlar 220 (ikiyüzyirmi) VAC +%10 (on), 50 (elli) Hz %5 (beş) elektrik gücünde sıhhatli olarak çalışacaktır.
- ÜRÜN' ü oluşturan tüm parçalar, lisansın alındığı dönem süresince (1/3 yıl) parça dahil yerinde garanti güvencesine sahip olmalıdır. Garanti süresi içinde oluşacak arıza durumunda, FİRMA ÜRÜN'ü engeç 24 saat içinde KURUM' dan teslim alacaktır. En geç 48 saat içinde bedelsiz olarak arızayı giderip BT'ye teslim edecektir.

YETKİNLİK – YETERLİLİK

FİRMA, başvuru evraklarıyla birlikte aşağıdaki belgeleri de sunacaktır.

- Akredite Satış Yöneticisi - Palo Alto ASE (Accredited Sales Executive)
- Cisco CCIE Security
- Security Engineer
- Cisco Certified Specialist - Data Center Core
- Yetki Belgesi
- ISO 27001 Bilgi Güvenliği Yönetim Sistemleri
- ISO 9001:2015 veya eşdeğer kalite uygunluk belgesi (TS13242 veya TS12739)
-

TEKNİK ÖZELLİKLER

Yeni Nesil Veri Merkezi Güvenlik Duvarı 2 Adet

Teklif edilen cihazlar donanım temelli olarak çalışacak şekilde teklif edilecektir. Harici switch veya yük dengeleyici ile çözümler kabul edilmeyecektir.

Cihazlar üzerindeki lisanslar 3 yıllık teklif edilecektir.

Cihazların merkezi olarak yönetilebileceği ve merkezi olarak logların toplanabileceği yazılım teklif edilecektir.

Cihazlar üzerinde ASIC veya FPGA bulunacaktır. Ayrıca cihaz üzerinde 24 core CPU olacaktır.

Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, son 10 yıl için "Enterprise Firewall" "Gartner Magic Quadrant" tablosunda Liderler alanında yer almalıdır.

Cihazın kendi üzerindeki Yönetim ve paket işleme katmanları birbirinden bağımsız olacaktır. Yönetim katmanın kendine ait dedike CPU ve RAM kaynağı olmalıdır. Bu kaynak sonradan atanabiliyorsa cihaz performansına etkisi olmamalıdır.

Cihaz üzerindeki Yönetim katmanı (management plane) restart/reboot edildiğinde dahi paket işleme katmanı (data plane) kesintisiz paket kaybı olmadan çalışmaya devam edecektir.

Her bir cihaz üzerinde en az 8 adet 1/2.5/5/10 Gbps Bakır port, en az 12 adet 1/10 Gbps SFP+ fiber yuvası, en az 4 adet 1/10/25G ve en az 4 adet 40/100G QSFP28 port bulunmalıdır.

Teklif edilecek cihaz üzerinde en az 480GB SSD disk bulunacaktır.

Cihaz üzerinde yedeklilik (HA) ve yönetim (management) için cihaz üzerinde verilmesi istenen data (ağ) portlarından ayrı şekilde cihaz üzerinde yer alacaktır.

Teklif edilecek iki cihaz birbirleri arasında IPv4/IPv6 aktif-pasif yedekli mimaride çalışmayı desteklemelidir.

Cihaz Uygulama kontrolü ve cihaz üzerinde loglama açıkken en az 52 Gbps performans sağlamalıdır. Bu değer enterprise ortam değerleri (appmix, enterprise mix) ile ölçülmüş olmalıdır.

Teklif edilen güvenlik duvarının atak önleme (Application Control, IPS, Anti-Virüs, Anti-spyware ya da Anti-Bot, Dosya uzantısına göre engelleme, 0. Gün Saldırıları (APT) Tespit ve Analiz ve cihaz üzerinde loglama) özellikleri aynı anda çalışır iken enterprise ortam değerleri ile (appmix, enterprise mix) en az 35 Gbps performans sağlamalıdır. Bu değerler üreticinin herkese açık olan web sitesinden yayınlanmış olmalıdır.

IPsec VPN throughput değeri en az 20 Gbps olacaktır. Bu değer 64KB HTTP paketleri ölçülmüş olmalıdır.

Anlık olarak en az 5.000.000 oturum destekleyecektir. Saniyede en az 270.000 yeni oturum açma kapasitesine sahip olacaktır. Bu değer 1 byte http paketleri ile ölçülmüş olmalıdır.

Cihaz üzerinde yedekli güç kaynağı ve fanlar olacaktır. Güç kaynakları ve fanlar hotswap mimarisinde çalışacaktır.

Cihaz üzerinde en az 20 adet sanal router ve en az 10 adet sanal firewall oluşturulacak şekilde teklif edilecektir.

Cihaz, mimari açıdan stateful inspection, IP Paket Filtreleme ve Uygulama Tanıma özelliklerini bünyesinde bulundurmalı ve aşağıdaki güvenlik servislerine sahip olmalıdır.

a. Firewall
b. IPSEC VPN, SSL VPN
c. Uygulama kontrolü (Application Control)
d. Kullanıcı kimliği entegrasyon özelliği
e. SSL çözme ve yönlendirme
f. URL Filtreleme

Cihaz QoS destekleyecektir. Kullanıcı adı/grubu, hedef/kaynak IP, Url kategoriye göre ve uygulama bazında bant genişliği sınırlaması yapabilmelidir. Ayrıca Trafik önceliklendirme yapabilecektir. Cihaz DSCP marking yapabilecektir.

En az 4000 adet VLAN desteği olmalıdır. Güvenlik Duvarı LLDP (Link Layer Discover Protocol) protokolünü desteklemelidir. Böylece cihaz kendine bağlı diğer cihazlar ile ilgili bilgileri (Mac adresi, sistem adı, kendine bağlı port ile ilgili bilgileri) sunabilmelidir.

Güvenlik Duvarının 802.3ad LACP, SNMPv3 ve DHCP-server özellikleri olacaktır.

Güvenlik Duvarının Netflow desteği olmalıdır. Fiziksel port bazında netflow profili tanımlanabilmelidir.

Güvenlik duvarı openconfig, XML API ve REST API gibi otomasyon teknolojilerini destekleyecektir.

Path monitoring vb özelliği cihaz üzerinde tanımlanan statik route tanımları bağdaştırılabilecektir. Böylece tanımlanan statik yönlendirmeler üzerinden sağlanan erişimlerin çalışıp çalışmadığını kontrol edebilecektir. Erişim olmadığı durumlarda statik yönlendirme satırını yönlendirme tablosundan otomatik olarak kaldırarak alternatif yoldan erişim imkânı sağlanacaktır.

Cihaz üzerinde IPv4/v6 politika tabanlı yönlendirme yapılabilecektir.
Cihazlar IPv4 ve IPv6 IPsec destekleyecektir.
Cihaz üzerindeki portlar Layer3 (routing mod) ve Layer2 (bridge mod), Layer 1 (vwire mod - saydam) ve Monitoring (TAP mod) katmanlarında çalışabilecektir. Cihaz üzerindeki farklı portlar cihaz modu değiştirmeden, aynı ön tanımlı sanal güvenlik üzerinde farklı port modlarında (L3, L2, L1, Tap) çalışabilecektir. Cihazın yeniden başlatılmasına gerek kalmadan üzerindeki portların çalışma seviyesi istendiği gibi değiştirilebilmelidir.
Cihazın Multicast yönlendirme desteği olmalı ve PIM-SM, PIM-SSM, IGMP v1, v2, v3 desteklemelidir. Ayrıca RP (Rendezvous Point) olarak çalışacaktır.
Cihaz GRE tunnel destekleyecektir.
Cihazın yeniden başlatılmasına gerek kalmadan üzerindeki portların çalışma seviyesi (L2/L3, saydam, monitoring) istendiği gibi değiştirilebilmelidir.
MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılabilecektir. Cihaz kullanıcı adı bilgilerini birden fazla yöntem ile (syslog, XML API, Active directory, XFF gibi) aynı anda dış kaynaklardan alıp kullanabilecektir.
Güvenlik duvarı üzerinde etiketleme yöntemi ile dinamik kullanıcı grupları oluşturulabilecektir.
Cihaz SSL VPN, captive portal ve çok faktörlü koruma servislerinde kimlik doğrulamak için Ldap, Radius, saml gibi protokolleri destekleyecektir.
Cihaz üzerinde en az 3000 (üçbin) uygulamayı tanıyabilen uygulama kontrol özelliği olacaktır. Cihaz ara yüzünden bu değer gösterilecektir. Uygulama imzaları elle yüklenebilecektir.
Cihaz üzerinde aşağıda belirtilen SSL VPN özelliği olmalıdır.

a. Windows, MACOS cihazlar için SSL VPN istemcileri desteklemelidir.
b. En az 15.000 SSL VPN bağlantısını destekleyecektir.
c. VPN için Detaylı loglama ve raporlama ara yüzü sunacaktır.
d. Kullanıcı oturum açma (her zaman açık), Talep üzerine, Oturum Öncesi (her zaman açık), Oturum öncesi, ardından isteğe bağlı, Kullanıcı tarafından başlatılan oturum öncesi bağlantı metotlarını destekleyecektir.

Cihaz üzerinde elle URL listeleri oluşturulabilecektir. Bu liste ile URL filtreleme yapılabilecektir.
Inbound (giriş) ve Outbound (çıkış) yönünde HTTPS inspection yapabilecektir. TLS 1.2 ve TLS 1.3 decryption desteği olacaktır. HTTP/2 uygulamaları için bütün kontrol özelliklerini kullanabilecektir. (App-control, IPS, AV, dosya bloklama vb .). HTTPS trafiğinin incelenebilmesi için gerekli olan Sertifika cihaza dışardan yüklenebilecektir. Aynı zamanda cihaz üzerinde üretilen bir self-signed SSL sertifika da bu amaç için kullanılabilecektir. Cihaz kendi üzerinde self-signed CA root sertifika üretecektir.
Teklif edilecek cihaz kendi üzerinde tüm yönetim fonksiyonlarını gerçekleştirebilecek WEB ara yüzü sunabilecektir. Cihaz kendi üzerinde loglama ve raporlama sağlayabilecektir. Kurum için özelleştirilmiş raporlar oluşturulabilecektir.
Güvenlik duvarı üzerinde Yedeklenen kurallar ve konfigürasyon yeniden başlatmaya ihtiyaç duymadan geri yüklenip aktif hale getirilebilecektir.
Coğrafi bölgelere veya Ülkelere göre güvenlik kuralları uygulanabilecek; bir kurala birden çok coğrafi bölge veya Ülke eklenebilecektir. Böylece belirli uygulama trafikleri istenen ülkeler için engellenebilecektir
Cihaz güvenlik kuralı bazında dosya tipine göre ve engelleme yapabilecektir.
Mevcut cihazlardan Politika geçişlerini ve kural optimizasyonunu yapacak servis ve yazılımlar ücretsiz olarak sağlanacaktır. Lisans gerekiyorsa bu servisler için teklife dahil edilecektir.
Teklif edilen Cihazlar Network Packet ve SSL broker olarak çalışabilecektir.

a. Kural bazlı olarak TCP, UDP paketlerini farklı cihazlara gönderip alabilecektir. Zone, kaynak/hedef IP, Uygulama ve kullanıcı kimliği bazlı olarak paketleri farklı üçüncü taraf trafik işleme cihaz ya da sistemlerine (IPS, Network Forensic, Sandbox vb.) gönderebilmelidir.

b. Cihazlar, üzerine gelen istemci tabanlı ve sunuculara doğru gelen web SSL trafiğini decrypt edebilmeli ve decrypt ettiği bu trafiği üçüncü taraf trafik işleme cihaz ya da sistemlerine (IPS, Network Forensic vb.) gönderebilmelidir. Bahse konu üçüncü taraf cihaz ya da sistemler, trafik üzerinde gerekli işlemleri gerçekleştirdikten sonra teklif edilecek cihazlar bu trafiği üçüncü taraf cihaz ya da sistemlerden geri alıp tekrar encrypt ederek trafiğin yoluna devam etmesini sağlayabilmelidir.

Güvenlik duvarı üzerindeki yönetim ara yüzünde güvenlik kurallarını uygulama katmanı seviyesinde güncelleme ve politika optimizasyonu yapabilmek için aşağıdaki özelliklerin bulunması gerekmektedir.

a. Uygulama imzası tanımlanmamış kurallar ve bu kurallardan geçen uygulamaları son 7, 15 ,30 gün e göre raporlayabilecek ve listenen uygulama imzaları istenilenler seçilerek kuralda aktif hale getirebilecektir.
b. Fazladan tanımlanmış uygulama imzası olan kuralları raporlayabilecektir. Kuraldan geçen uygulama imzalarını son 7, 15 ,30 gün e göre raporlayabilecektir.
c. Kurallardan geçen uygulamaların ilk ve son geçiş tarihi ve son 30 günde ne kadar bant genişliği tükettiği bilgisini raporlayabilecektir.
d. Son 30 gün, 90 gün de kullanılmayan kuralları raporlayabilecektir.

Cihaz üzerinde aşağıda iletilen URL filtreleme özelliği olmalıdır.

1) URL filtreleme özelliği Active Directory ile entegre çalışabilecek bu sayede Active Directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında URL filtreleme kuralları tanımlanabilecektir.
2) Güvenlik duvarı ara yüzünden istenilen URL ler için tekrar kategorilendirme talebi girilebilmelidir.
3) Gerçek zamanlı Web tehdidi önleme modülü ile yeni ve gelişen, daha önce görülmemiş tehditlere (ör. kimlik avı, exploits, dolandırıcılık(fraud), C2) karşı koruma sağlayacaktır
4) Atlatma önleme modülü ile Gizleme(cloacking), sahte CAPTCHA'lar ve HTML karakter kodlaması gibi kaçma tekniklerine karşı koruma sağlayacaktır.
5) Güncel zararlı yazılımların eriştiği C&C (Command and Control) ve Malware Download URL listelerini dinamik olarak güncelleyebilmelidir.
6) Gerçek zamanlı analiz yaparak kimlik hırsızlığına karşı pishing sitelerini ve Java script tabanlı atakları engelleyebilecektir.
7) İmaj Algılama modülü ile web sayfalarındaki görüntüleri analiz edip kimlik avı girişimlerinde yaygın olarak kullanılan markaları taklit edip etmediklerini belirleyebilmeli ve engelleyebilmelidir.
8) URL kategorilerini kullanarak security policy match kısmında kullanılabilmeli ve URL kategorisi için farklı bant genişliği sınırlandırma politikaları yazılabilmelidir.
9) URL leri yüksek (son 30 gün içerisinde url ile ilgili zararlı aktivite bulunması) ve orta riskli (son 60 gün içerisinde url ile ilgili zararlı aktivite bulunması) olarak kategorize edebilecektir.
10) Son 32 günde kayıt edilmiş URL leri (new registered domain) kategorize edebilecektir.
11) Erişilen URL ler in detaylı olarak logları tutulabilecek ve syslog ile harici sistemlere aktarılabilecektir.

12) Oltalama (phishing) saldırılarına karşı, kullanıcı kimlik kontrol özelliği olacaktır. Önerilecek çözüm ile HTTP/HTTPS POST seviyesinde kullanıcı ve şifre bilgilerinin gönderilmesini/çalınmasını engelleyebilmelidir. Kullanıcı kimlik bilgilerinin kontrolünü Active Directory ile entegre bir şekilde yapabilmelidir. Bu özellik için gerekli aynı üreticiye ait yazılım, lisans vb bilşenler teklife dahil edilecektir.
13) Dil çeviri web sitelerine (ör. Google Çeviri) girilen URL'lere URL Filtreleme politikaları uygulayabilecektir.
14) Son kullanıcılar web aramalarının ve internet arşivlerinin önbelleğe alınmış sonuçlarını görüntülemeye çalıştığında URL Filtreleme politikaları uygulanabilecektir.
15) Güvenli Arama (safe-search - Google, Yandex, Yahoo veya Bing) özelliği ile Kullanıcıların arama sonuçlarında uygunsuz içeriğin görüntülenmesi engellenebilecektir.
16) Cihaz üzerinde detayları aşağıda belirtilen IPS özelliği olmalıdır.
    a. Farklı kullanıcı veya kullanıcı grupları için farklı IPS politikaları oluşturulabilmelidir.
    b. Cihaz üzerindeki IPS imzaları CVE id lerine, kritiklik seviyelerine ve host (client/server) tipine göre aranabilecektir.
    c. IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza için ayrı ayrı ayarlanabilmelidir. İmzalarda farklı aksiyonlar alınabilmelidir. IP bloklaması kaynak IP ve hem kaynak hem hedef IP bazında yapılabilecektir.
    d. 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.
    e. Önerilecek IPS fonksiyonunda saldırı imzalarına bağımlı kalmaksızın saldırıları engelleyen Protokol Anormallik Tespiti (Protocol Anomaly Detection) teknolojisine sahip olacaktır.
    f. Inline derin öğrenme algılama modelleri aracılığıyla gerçek zamanlı trafik incelemesini kullanarak kaçınma amaçlı komuta ve kontrol (C2) tehditlerine karşı koruma sağlaması gerekmektedir.
    g. IPS fonksiyonu aşağıdaki saldırı tiplerine karşı koyabilmelidir;
        - Brute Force
        - Code/Command execution
        - Sql-injection
        - Exploit-kit
        - Denial of Service
        - Info-leak
        - Overflow
        - Scan

46) Cihaz üzerinde detayları aşağıda belirtilen Anti-Spyware tespit ve engelleme özelliği olmalıdır.
    a. Port ve protokolden bağımsız çalışmalı, internete doğru yapılan tüm ip trafiğini inceleyebilmelidir.
    b. Bilinen botnet'ler için imza temelli bloklama yapabilmelidir. Her bir botnet imzası için alınabilecek aksiyonlar sistem yöneticileri tarafından konfigüre edilebilmelidir.
    c. İmzalarda farklı aksiyonlar alınabilmelidir.
    d. Farklı kullanıcı veya kullanıcı grupları için farklı Anti-spyware politikaları oluşturulabilmelidir.

e. Botnet fonksiyonu aşağıdaki saldırı tiplerine karşı koyabilmelidir;

- Adware
- Botnet
- Backdoor
- Browser-Hijack
- Data-theft
- keylogger
- spyware
- net-worm
- p2p-communication

47) Cihaz üzerinde detayları aşağıda belirtilen Anti-Virüs ve Anti-Malware tespit ve engelleme sistemi olmalıdır.

a. Bilinen virüsler için imza temelli bloklama yapabilmelidir.

b. Anti-virüs imzaları payload tabanlı olmalıdır, hash tabanlı olmamalıdır.

c. Akan dosya trafiğini tarayabilmelidir. Arşivlenmiş dosyaları tarayabilmelidir.

d. FTP, HTTP, HTTP2, SMB, POP3, IMAP protokolleri üzerinden transfer edilen zararlı dosyaları engelleyebilecektir.

e. Anti-virüs mimarisi Active Directory ile entegre çalışabilecek bu sayede Active Directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında Anti-virüs kuralları tanımlanabilecektir.

f. Farklı kullanıcı veya kullanıcı grupları için farklı Anti-virüs politikaları oluşturulabilmelidir.

KURUM	**FİRMA**
İSTANBUL BİLGİ ÜNİVERSİTESİ	