**KUŞADASI BELEDİYE BAŞKANLIĞI**
**BİLGİ İŞLEM MÜDÜRLÜĞÜ**
**( FİREWALL-FW CİHAZI ) GÜVENLİK DUVARI TEKNİK ŞARTNAME**

**GÜVENLİK DUVARI ( FW )**

1) Tüm Güvenlik Duvarları aynı üreticiye ait olacak ve donanımsal olarak teklif edilecektir, teklifler 3 yıllık olacaktır.
2) Teklif edilen çözüm donanım temelli olarak çalışacak 1 (bir) adet ürün olarak teklif edilecektir.
3) Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, son 10 (on) yıl için "Enterprise Firewall" "Gartner Magic Quadrant" tablosunda Liderler alanında yer almalıdır.
4) Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, "NSS Labs Network IPS" ve "NSS Labs Next Generation Firewall" testlerine girmiş olması gereklidir.
5) Cihaz üzerinde en az 8 (sekiz) adet 10/100/1000Mbps Bakır port yuvası bulunmalıdır. Ve harici olarak magement portu bulunmadır.
6) Cihazlar Uygulama kontrolü açıkken en az appmix/enterprise mix test koşullarında 4,4 Gbps performans sağlamalıdır.
7) Teklif edilen güvenlik duvarının atak önleme (Application Control, IPS, AV, Anti-spyware) özellikleri aynı anda açık appmix/enterprise mix test koşullarında 2,4 Gbps performansı desteklemelidir.
8) IPsec VPN throughput değeri en az 3 Gbps olacaktır. Cihaz üzerinde en az 2800 adet tünel tanımlanabilecektir.
9) Anlık olarak en az 400.000 oturum destekleyecektir.
10) Saniyede en az 73.000 yeni oturum açma kapasitesine sahip olacaktır.
11) Teklif edilecek cihaz üzerinde 128 GB eMMC veya SSD kapasiteli disk olacaktır.

1) Cihaz üzerinde belirtilen SSL VPN özelliği olmalıdır.
    a. Windows, MACOS cihazlar için IPv4 ve IPv6 için SSL VPN istemcileri desteklemelidir.
    b. En az 15.00 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.
    e. IOS, Android ve Linux clientlar için SSL VPN bağlantısı destekleyecektir.
    f. Ajansız SSL VPN desteği olacaktır.
    g. SSL-VPN ile bağlanan kullanıcıların bağlandıkları cihazlar üzerinde politikalar uygulanabilecek ve en az antivirüs varlığı ve/veya güncelliği, işletim sistemi güncelliği, belirli uygulamaların yama kontrolünün, firewall

servisinin çalışması, disk backup ve disk encryption servis kontrolleri yapılacaktır.

h. Rota, domain ve uygulama için split tunneling uygulanabilecektir.
i. Desteklenen bütün clientlar üzerinde Çok faktörlü kimlik doğrulama destekleyecektir.
j. SAML, Kerberos, Radius, Client sertifikası, Lokal database ve LDAP otantikasyon servislerini destekleyecektir.
k. Zararlı aktivite tespiti durumunda Cihazları kullanıcı adı , IP den bağımsız şekilde bağlanmasını otomatik engelleyebilecektir.
l. Oturumlardan önce ve sonra script çalıştırılmasını sağlayabilmelidir.

12) Cihaz üzerinde yedekli güç kaynağı olacaktır .
13) Cihazlar, mimari açıdan stateful inspection, IP Paket Filtreleme ve Uygulama Tanıma özelliklerini bünyesinde bulundurmalı ve aşağıdaki güvenlik servislerine sahip olmalıdır.
    a. Yeni Nesil Firewall
    b. IPSEC VPN, SSL VPN
    c. Uygulama kontrolü (Application Control)
    d. URL Filtreleme
    e. DNS Güvenliği
    f. Atak Engelleme (IPS)
    g. Anti-Virus
    h. Anti-Spyware
    i. AD (active directory) entegrasyon özelliği olmalıdır.
    j. Sıfırıncı gün koruması
14) Saat, gün, tarih, periyot bazında erişim kontrolü yapabilmelidir.
15) OSI Layer-4 ile Layer-7 arasındaki ağ trafiğini izleyebilmelidir.
16) 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.
17) NAT kuralları, Güvenlik kurallarından bağımsız ayrı kural seti olarak tanımlanacaktır.
18) Güvenlik duvarı Zone tabanlı çalışmalıdır. Birden fazla interface / sub-interface aynı zone altına tanımlanabilmelidir. Güvenlik ve NAT kuralları zone tabanlı oluşturulabilmelidir.
19) DHCP server ve IPv4/v6 DHCP Relay olarak yapılandırabilecektir.
20) Güvenlik Duvarı 802.3ad LACP desteklemelidir.
21) Güvenlik Duvarı SNMPv3 desteklemelidir.
22) Güvenlik Duvarının Netflow desteği olmalıdır. Fiziksel port bazında netflow profili tanımlanabilmelidir.

23) Sistem IPv4/v6 Statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerini desteklemelidir, lisans gerekiyorsa teklife dahil edilmelidir.
24) Path monitoring 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 ototmatik olarak kaldırarak alternative yoldan erişim imkanı sağlanacaktır.
25) Güvenlik Duvarı BFD (Bidirectional Forward detection) özelliğine sahip olmalıdır. Böylece yönlendirme seviyesinde oluşabilecek herhangi bir değişiklikte daha hızlı adaptosyon sağlanabilecektir.
26) Cihazın Multicast yönlendirme desteği olmalı ve PIM-SM, PIM-SSM, IGMP v1, v2, v3 desteklemelidir.
27) Site to site ve client to site IPSEC VPN desteği olmalıdır.
28) Cihazlar, IPSec VPN standardını desteklemelidir. IKE şifreleme şemalarını desteklemelidir. 3DES , AES algoritmaları ile paket şifreleme yapabilmelidir. Veri bütünlüğü için MD5 ve SHA1 algoritmalarını desteklemelidir. Diffie-Hellman groups 1, 2 ve 5 (Perfect forward secrecy) desteği olmalıdır.
29) Cihazlar IPv6 IPsec destekleyecektir.
30) Layer3 (routing mod) ve Layer2 (bridge mod), Layer 1 (Saydam mod) ve Monitoring (TAP mod) katmanlarında çalışabilecektir. Cihaz üzerindeki farklı portlar aynı anda aynı sanal firewall üzerinde olsa dahi farklı port modlarında çalışabilecektir.
31) Cihazın yeniden başlatılmasına gerek kalmadan üzerindeki portların çalışma seviyesi (L2/L3, saydam, monitoring ) istendiği gibi değiştirilebilmelidir.
32) MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılabilecektir. Kullanıcıya göre kural yazma sadece kimlik bilgisi gönderen uygulamalarla sınırlı olmayacaktır. Tutulan kayıtlarda kullanıcı ismi de yer alacaktır.
33) Kullanıcı entegrasyonu için yönetici (administrator) hesabına ve Active Directory yapısında her hangi bir değişikliğe ihtiyaç olmayacaktır.
34) Cihaz kendisine otantikasyon yapan sistemlerin gönderdiği syslog mesajlarını çözerek User-IP mapping desteği olacaktır.
35) Cihaz XML-API arayüzünden 3üncü parti (wireless controller vb) kullanıcı doğrulaması yapan sistemlerden kullanıcı adı bilgilerini alabilecek API arayüzüne sahip olmalıdır.
36) Cihaz üzerinde en az 3500 uygulamayı tanıyabilen ve detayları aşağıda belirtilen uygulama kontrol özelliği olacaktır.
    a. Uygulama kontrol özelliği active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında uygulama kontrol kuralları tanımlanabilecektir.
    b. Veritabanında yer alan uygulamaların listesi, ilgili uygulamanın yer aldığı ana ve alt kategoriler, ilgili uygulamanın risk seviyesi bilgileri yönetim ekranında görüntülenebilecektir.
    c. Uygulama bloklama ve uyarı portalı değiştirilebilecektir.

d. Kuruma özel uygulamaların sisteme tanıtılması özel imza oluşturmak suretiyle mümkün olmalıdır.

e. Bilinmeyen uygulamaları, Unknown-TCP ve Unknown-UDP olarak tanımlayabilmeli ve wireshark gibi araçlar ile içeriğini gösterebilecek şekilde yakalayabilmelidir.

37) 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 Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip gibi 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. IPS fonksiyonu aşağıdaki saldırı tiplerine karşı koyabilmelidir;

- Brute Force
- Code/Command execution
- Sql-injection
- Exploit-kit
- Denial of Service
- Info-leak
- Overflow
- Scan

38) 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. Botnet komuta kontrol merkezlerine erişim için yapılan adres çözümleme isteklerini tespit ve dns sorgusu esnasında trafiği bloklayabilme ve özelliğine sahip olmalıdır.
c. Cihazın DNS Sinkhole özelliği ile, kötü domain isteklerini yönetici tarafından atanmış IP adresine çözülmesini sağlayabilmelidir. Böylelikle sistem üzerinde enfekte olmuş sistemler kolyaca tespit edilebilecektir.
d. Bilinen botnet'ler için imza temelli bloklama yapabilmelidir. Her bir botnet imzası için alınabilecek aksiyonlar sistem yöneticileri tarafından konfigüre edilebilmelidir.
e. İmzalarda Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip gibi aksiyonlar alınabilmelidir.
f. Farklı kullanıcı veya kullanıcı grupları için farklı Anti-spyware politikaları oluşturulabilmelidir.
g. Botnet fonksiyonu aşağıdaki saldırı tiplerine karşı koyabilmelidir;
    - Adware
    - Botnet
    - Backdoor
    - Browser-Hijack
    - Data-theft
    - keylogger
    - spyware
    - net-worm
    - p2p-communication

39) Cihaz üzerinde detayları aşağıda belirtilen Anti-Virüs tespit ve engelleme sistemi olmalıdır.
    a. Bilinen virüsler için imza temelli bloklama yapabilmelidir.
    b. Akan dosya trafiğini tarayabilmelidir. Arşivlenmiş dosyaları tarayabilmelidir.
    c. Anti-virüs mimarisi active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında Anti-virüs kuralları tanımlanabilecektir.

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

40) Cihaz üzerinde aşağıda iletilen URL filtreleme özelliği olmalıdır.

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

l. 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.

m. Dil çeviri web sitelerine (ör. Google Çeviri) girilen URL'lere URL Filtreleme politikaları uygulayabilecektir.

n. Son kullanıcılar web aramalarının ve internet arşivlerinin önbelleğe alınmış sonuçlarını görüntülemeye çalıştığında URL Filtreleme politikaları uygulanabilecektir.

o. Güvenli Arama (safe-search - Google, Yandex, Yahoo veya Bing) özelliği ile Kullanıcıların arama sonuçlarında uygunsuz içeriğin görüntülenmesi engellenebilecektir.

41) Cihazın Data filtreleme özelliği olacak ve kural tabanlı çalışacaktır. Dosya türü, keyword, regex özelliklerini sağlamalıdır. Bunun için gerekli lisanslar teklife dahil edilecektir.

42) Önerilecek sistem dosya transferleri aracılığıyla gerçekleştirilebilecek 0.gün (zero-day) ve gelişmiş kalıcı tehdit (Advanced Persistent Threats) saldırılarına karşı aşağıdaki özellikleri desteklemelidir.

a. Güvenlik duvarı bulut sandbox ile 0. Gün zararlıları tespit edebilmeli, bulut üzerindeki analiz servislerini aynı anda kullanabilmelidir.

b. APT çözümü şüpheli dosyaları.çalıştırılabilir (exe ve .dll) uzantılı dosyaları, virus yada malware imzalarınca tespit edilemeyen bilinmeyen zararlı içerikleri analizini yapabilmelidir.

43) Yazılımın üzerinde aşağıda iletilen DNS Güvenliği özellikleri olmalıdır. Bu özellikler NGFW üzerinde sağlanamıyor ise ilave yazılım ve lisans teklifleri kabul edilecektir.

a. DNS güvenlik özelliği Kurumun DNS altyapısında herhangi bir değişikliğe ihtiyaç olmadan Güvenlik duvarı üzerinde aktif edilebilecektir.

b. DNS güvenlik özelliği Makine öğrenmesi destekli olması gerekmektedir.

c. DNS güvenlik özelliği DGA (Domain Generation algorithm) ve DNS tünellemelerini engelleyecektir.

d. DNS güvenlik özelliği ile zararlı DNS isteklerini yapan client lar tespit edilebilecektir. Tesbit edilen kullanıcıların güvenlik duvarı üzerinden sunuculara / internete erişimleri otomatik olarak engellenebilecektir.

e. Ultra-slow DNS tünellemelerine Karşı koruma sağlayacaktır.

f. DNS rebinding ataklarına karşı koruma sağlayacaktır.
g. Dangling DNS atakalarına koruma sağlayacaktır.
h. Dictionary DGA ve fast flux domain lere karşı koruma sağlayacaktır.
i. Kurumun DNS trafiğinin detaylı raporlamasını sağlayacaktır.
j. Yapılan DNS isteklerinin analizi bu raparlama sayfasında detaylı olarak sağlanacaktır. Yapılan Malware , DGA, tünelleme, C2 , Dynamic DNSi Yeni kayıt edilmiş domain isteklerinin raporlaması detaylı olarak sağlanacaktır.

44) Coğrafi bölgelere göre güvenlik kuralları uygulanabilecek; bir kurala birden çok coğrafi bölge eklenebilecektir.
45) Kullanıcı adı/grubu, hedef/kaynak IP ve uygulama bazında bant genişliği sınırlaması uygulanabilecektir.
46) Cihazın kendi web yönetim arayüzünde Kural çakışmasının önlenmesi için kural denetim özelliği olacaktır. Mevcut kuralları geçersiz kılan bir kural yazılması durumunda uyarı verecektir.
47) Cihaz yönetim arayüzü üzerinden Kural değişiklikleri güvenlik duvarına yüklenirken (commit/policy install/vb.) aktif kurallar otomatik olarak yedeklenebilecektir.
48) Yedeklenen kurallar yeniden başlatmaya ihtiyaç duymadan geri yüklenebilecektir.
49) Loglar SNMP, syslog, mail ile harici log yönetim sistemlerine gönderilebilecektir.
50) Kural bazında logları SNMP, syslog, mail ile harici log yönetim sistemlerine gönderilebilecektir.
51) Cihaz göndereceği loglar üzerinde özel tanımlanabilen filtereler uygulayarak bu filtrelere göre snmp, syslog ve email ile log gönderebilmelidir.
52) Coğrafi bölgelere ve Ülkelere göre güvenlik kuralları uygulanabilecek; bir kurala birden çok coğrafi bölge/Ülke eklenebilecektir. Böylece belirli uygulama trafikleri istenen ülkeler için engellenebilecektir
53) Cihaz üzerinde dinamik IP/URL/Domain adresi engelleme listeleri oluşturulabilecektir. Engellenecek IP adreslerinin listesinin tutulduğu URL den bu listeyi cihaz otomatik olarak alarak güvenlik duvarı üzerinde bu IP/URL/Domain adreslerin erişimini engelleyebilecektir.
54) Üretici firmanın siber istihbarat servisi üzerinde tespit ettiği zararlı IP lerin listesi Cihaz üzerinde sürekli güncellenebilecektir. Böylece bu IP lere erişimler engellenebilecektir.
55) SYN Flood, UDP Flood, ICMP Flood ataklarına karşı koruma sağlayacaktır. Sistem kaynaklarını korumak amacıyla farklı eşik seviyeleri (örneğin maks. eşzamanlı bağlantı sayısı vs.) tanımlanabilecektir.
56) Multipath tcp evasion larına karşı koruma sağlamalıdır.
57) Fragmante edilmiş paketleri tesbit edip bloklayabilecektir.
58) TCP port taramalarına karşı engelleme yapabilecektir.
59) Loglama ve raporlama modülüde teklife eklenmelidir.

Ertuğrul TEMEL
Bilgi İşlem Md. V.