AĞ GÜVENLİĞİ SD-WAN ÇÖZÜMÜ ALIMI
TEKNİK ŞARTNAMESİ
GENEL ŞARTLAR

1. Kurumumuzda çalışan, aşağıda listesi verilen Fortinet Güvenlik Sistemleri için güncelleme servisleri satın alınacaktır.
2. Kurumda Çalışan Fortinet Güvenlik Sistemleri

FortiGate-600E	Unified Threat Protection (UTP)
FortiGate-100F	Unified Threat Protection (UTP)
FortiAnalyzer-VM	24x7 FortiCare Contract (for 1-26 GB/Day of Logs)

3. Tüm donanım birimleri tamamen yeni ve hiç kullanılmamış olmalıdır. Tüm kurulumlar İdare'nin teknik personeli ile birlikte gerçekleştirilecektir.
4. Kurum bünyesinde bulunan listesi yukarıda verilmiş olan Fortinet ağ güvenlik sisteminin garanti süresinin bitiminden itibaren en az 3 YIL yazılım üretici güncelleme paketi teklife dahil edilmelidir.
5. Güvenlik sistemi için alınacak güncelleme servislerinin aşağıdakileri içermesi gerekmektedir:
   - 3 Yıl Süreli Firmware/Yazılım güncelleme
   - 3 Yıl Süreli Üretici firmadan 24x7 e-mail destek
   - 3 Yıl Süreli sınırsız kullanıcı için AntiVirus güncellemesi
   - 3 Yıl Süreli sınırsız kullanıcı için Uygulama Kontrol güncellemesi
   - 3 Yıl Süreli sınırsız kullanıcı için IPS güncellemesi
   - 3 Yıl Süreli sınırsız kullanıcı için URL Kategori Filtreleme güncellemesi
   - 3 Yıl Süreli sınırsız kullanıcı için AntiSpam güncellemesi
   - 3 Yıl Süreli sınırsız kullanıcı için Sandbox Cloud güncellemesi
   - 3 Yıl Süreli Donanım Garantisi
6. Firma teklif ettiği cihazlara ait ürünlerin üreticisinden veya yetkili distribütöründen almış olduğu yetki belgesini teklif dosyasında sunmalıdır.
7. Firma, teklif ettikleri ürünlere ait Marka Model listesini teklif dosyasında sunmalıdır.
8. Firma, teklifine, teklif ettiği marka cihazlarla ilgili orijinal (İngilizce) dilindeki katalogları teklif dosyasına koymalıdır.
9. **Teklif edilecek tüm ürünler, çözümler ve yazılımlar aynı marka olmalıdır ve birbirleri ile tam uyumlu olmalıdır.**
10. Yüklenici, garanti süresi içerisinde, gerek duyulabilecek her türlü yedek parça, bakım, onarım ve yapılandırma hizmetini, ayrı bir ücret talep etmeden, sistemin kurulu bulunduğu yerde verecektir (işçilik

içinde ayrı bedel talep edilmeyecektir).

11. Yüklenici ile İdare arasındaki anlaşmazlık durumunda İdarenin kararları belirleyici olacaktır.

12. Yüklenici firma kullanacak ürünlerin orijinal (İngilizce) dilindeki veya Türkçe teknik dokümanlarını ve marka model listesini üretici kodları ile idareye yer teslimi, sürecinde teslim etmelidir. Kurum istenildiği taktirde numune ürün talep edecektir.

13. İşin kabulü olmadan oluşacak ürün arızaları; tamir ve onarım yolu ile düzeltilmeyecek, aynı ürünün birebir yedeği olan kullanılmamış yeni ürün ile değiştirilecektir.

14. Aşağıda belirtilen tüm ürün ve yazılım sistemlerin en az 3 yıl yazılım ve destek garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

15. Yüklenici firma kurulacak cihazlar ile ilgili 3 gün eğitim verecektir.

İHTİYAÇ LİSTESİ

1. İhale kapsamında tedarik edilecek tüm kalemler İdarenin belirleyeceği adrese teslim edilecektir.

2. Bu şartname kapsamında teklif edilecek tüm ürünler ayrı ayrı tüm şartları asgari düzeyde karşılayacaktır.

3. İstekliler teklif etmiş oldukları ürünlerin fiyatlarını birim malzeme listesine göre vereceklerdir.

4. İş ve işlemlerin yürütülmesi sırasındaki her türlü nakliye, ulaşım, konaklama, montaj ve iletişim gibi giderler yükleniciye ait olacaktır.

1.Güvenli SD-WAN Çözümü Genel Özellikleri

Uç noktada hatların aktif/aktif bir şekilde güvenli SD-WAN mimarisi altında çalıştırmasını sağlayan, interface bağımlılığı olmayan, hat kalitesi ölçerek uygulama bazlı dinamik ve akıllı trafik dağılımı yapabilen, bantgenişiliği yönetimi sunan, ssl denetim yapabilen, bütün bu yapıyı merkezi olarak yönetme ve loglama imkanı sunabilen, altyapısında güvenlik bileşenleri (IPS, Antivirus, URL filtering) bulunduran bir çözüm hedeflenmektedir.

1.1. **SD-WAN**

1.1.1. Sistemin aşağıda detayları belirtilen SD-WAN özellikleri olmalıdır.

1.1.2. Ürün, birden fazla geniş alan ağı (WAN) bağlantısının (örneğin MPLS, ADSL/VDSL, LTE) trafik paylaşımı amacıyla aktif/aktif mimaride kullanımını desteklemelidir.

1.1.3. Birden fazla WAN bağlantısı tek bir sanal hat (virtual interface) gibi tanımlanabilmeli ve bu sanal hatta doğru kural (policy) ve rota (route) yazılabilmelidir.

1.1.4. SD-WAN hatlarının bağlantı kalitesi

a. http
b. ping
c. tcp-echo
d. udp-echo
e. twamp

protokolleri aracılığıyla gecikme (latency), paket kaybı (packet loss) ve sapma (jitter) yöntemleriyle takip edilebilmelidir.

Hat durum kontrollerine ait geçmişe yönelik bilgiler grafik üzerinden gösterilebilmelidir. Bu sayede ilgili hat üzerinde yakın geçmişe ait paket kayıp seviyesi, gecikme ve sapma değerleri görüntülenebilmelidir.

1.1.5. Trafik, SD-WAN hatları arasında aşağıdaki yöntemlere göre dağıtılabilmelidir:

a. Kaynak IP'ye göre dağılım
b. Kaynak ve hedef IP'ye göre dağılım
c. Oturum sayısı (session) bazında oransal dağılım
d. Hat bazında eşik değer belirleyerek (Spillover) dağılım
e. Trafik oranı bazında (volumetric) oransal dağılım

1.1.6. Özelleştirilmiş SD-WAN kuralları tanımlanabilmelidir. Böylece belirli kullanıcı/kullanıcı grubu, kaynak ip, hedef ip ve uygulama/uygulama kategorisi tanımına göre trafiğin;

a. Öncelikli hattan gönderilmesi sağlanabilmelidir. Örneğin kritik uygulamalar MPLS'ten, mail ve internet gibi bulk uygulamaların ADSL'den gitmesi sağlanabilmelidir. Burada belirli SLA değerleri tanımlanabilmelidir. Örneğin kritik uygulamalar MPLS'ten giderken gecikme/paket kaybı/jitter değeri belirli bir threshold'u geçerse trafik otomatik olarak hat kalite değerleri daha iyi olan ADSL hattına yönlenebilmelidir. MPLS hattı düzeldiği zaman trafik otomatik olarak MPLS'e dönebilmelidir.

b. Hat kalite testlerine (latency, packet loss ve jitter) göre daha yüksek kaliteye sahip hattan gönderilmesi sağlanabilmelidir.

c. Sadece belirli bir SLA kriterini (latency, packet loss ve jitter) sağlayan hatlara trafik load-balance edilebilmelidir.

d. Spesifik bir hattan gönderilmesi sağlanabilmelidir.

1.1.7. Uygulamalar bazında ön tanımlı SLA değerleri bulunmalıdır. Böylece uygulamaların hangi SLA değeri ile en iyi şekilde çalıştığı sağlanmaktadır.

1.1.8. Uygulama/uygulama kategorisi bazında spesifik SD-WAN kuralları tanımlanabilmelidir. Bu sayede örneğin Youtube/Voice/Video/Outlook/Windows Update gibi uygulama trafiklerinin belirli hat üzerinden yönlendirilmesi sağlanabilmelidir.

1.1.9. Uç noktada direk internet erişimi (local breakout) güvenlik politikaları uygulanarak sağlanmalıdır. Böylece uç nokta internet trafiği merkeze taşınmadan güvenli bir şekilde lokalden internete eriştirilebilmelidir.

1.1.10. Paket kayıplarını azaltmak ve bantgenişliğini daha iyi kullanmak için FEC (Forward Error Correction) teknolojisini desteklemelidir.

1.1.11. Sistem IPv6 trafikleri için de SD-WAN özeliğine sahip olmalıdır.

1.1.12. SD-WAN bağlantıları üzerinde istenirse otomatik IPSEC VPN tünel oluşturma yeteneğine sahip olmalıdır. SD-WAN konfigürasyonu esnasında hangi hatlar üzerinde VPN tünel yapılacağı seçilebilmeli ve bu sayede birden fazla SD-WAN hatları üzerinden tek bir hedefe otomatik VPN tanımlaması yapılabilmelidir.

1.1.13. Sistemin merkezi yönetim çözümü bulunmalıdır. Tüm uç lokasyonda bulunan SD-WAN cihazlarındaki konfigürasyonlar tek merkezden yönetilebilmelidir. Tüm cihaz parametreleri,

güvenlik politikaları, SD-WAN politikaları, ipsec vpn ayarları merkezden grup bazlı ya da cihaz bazlı tek tek yapılabilmedir.

1.1.14. Merkezi yönetim sisteminde oluşturulacak uç nokta template konfigürasyonlar için orchestration çözümü olmalıdır. Uç nokta cihaz parametrelerini (ip, adsl user/password, routing gibi) bir tablodan (txt, excel) okuyarak merkezi yönetim sisteminde, API vasıtasıyla, otomatik olarak uç nokta template konfigürasyonlarının oluşturması sağlanmalıdır.

1.1.15. Merkezi yönetim sisteminde, sahada bulunan tüm SD-WAN cihazları bir harita üzerinde gösterilebilecektir. Hat kalite durumları anlık olarak görüntülenebilecek, cihazların durumları farklı renklerde gösterilmelidir.

1.1.16. Merkezi yönetim sisteminde, ölçülen hat kalitesi değerleri (paket kaybı, gecikme, sapma) geçmişe dönük gösterilmelidir.

1.1.17. Merkezi yönetim sisteminde meydana gelebilecek olumsuz bir duruma karşı sahada bulunan tüm cihazlar hiçbir fonksiyonunu kaybetmeden çalışmaya devam etmelidir. Cihazlarda konfigürasyon değişiklikleri cihaz arayüzleri üzerinden yapılabilmeli, yapılan değişiklikler otomatik olarak merkezi yönetim sistemine aktarılabilmelidir.

1.1.18. Çözüm ZTP'yi (Kolay Kurulum) desteklemelidir. Aşağıdaki yöntemlerle ZTP yapabilmelidir.

a. Uç noktaya gönderilen bir cihaz, lokalde bir switch portuna bağlanarak, DHCP'den otomatik olarak merkezi yönetim sunucusunun ip'sini alabilmelidir (DHCP option 240 sayesinde). Mevcut hatları kullanarak merkezden konfigürasyonunu otomatik olarak çekebilmelidir. Aynı şekilde uç noktaya gitmeden de cihazın genel müdürlük binası lokal network'ünde de aynı yöntemle konfigürasyonunu merkezi yönetim sunucusundan otomatik çekebilmelidir.

b. Cihazın internet erişiminin sağlanarak bulut üzerinden otomatik olarak merkezi yönetim sunucu bilgisini alması ve konfigürasyonu merkezi yönetim sunucusu üzerinden otomatik olarak çekmesi sağlanabilmelidir. Bu sayede uzak lokasyonlara kurulum işleminin sadece internet erişiminin sağlanmasıyla yapılabilmesi mümkün olmalıdır.

1.1.19. Sistemin merkezi log toplama ve raporlama çözümü olmalıdır. Tüm uç noktalardan gelen loglar merkezi olarak görüntülenmeli ve ihtiyaç duyulan raporlama yapılabilmelidir.

1.1.20. Merkezi olarak kullanıcı/kullanıcı grubu, kaynak ip/ağ, hedef ip/ağ ve uygulama bazlı bantgenişliği yönetim (QoS) desteği olmalıdır. Grup bazlı ya da uç nokta bazlı QoS yapılabilmelidir. QoS interface tabanlı, inbound/outbound yönünde ve zamana bağlı olarak hat kapasitesinin yüzdesel oranında tanımlanabilmelidir. Ses/video gibi kritik uygulamalara öncelik (priority) ve garanti bantgenişliği yazılabilmelidir. Belirlenen trafik için maksimum bantgenişliği tanımlama imkanı olmalıdır.

1.1.21. SSL inspection (https trafiğinin açılması) desteği olmalıdır. Bu sayede ssl trafiklerini açarak, uygulama detaylarına göre; SD-WAN, QoS, uygulama kuralları yazılabilmelidir.

1.1.22. Merkeze ulaşan trafiğin aynı interface'den geri dönmesi sağlanmalıdır. Örneğin kritik uygulamalar merkeze MPLS hattan ulaştı işe geri dönüş trafiğinin de MPLS hattan uç noktaya iletilmesi sağlanmalıdır.

1.1.23. Uç nokta lokalinde oluşturulacak Vlan'lar sayesinde segmentasyon yapılabilmeli, VLAN'lar arasında trafik kontrolü için güvenlik politikaları yazılabilmelidir.

1.1.24. Önerilecek SD-WAN çözümü, güncel "NSS Labs SDWAN" testlerinden 'Recommended' sertifikası almış olması gereklidir.

1.2. Uygulama Kontrol (Application Control)

1.2.1. Sistem üzerinde detayları aşağıda belirtilen uygulama kontrol özelliği bulunmalıdır.

1.2.2. Sistemin uygulama kütüphanesinde en az 2500 (ikibinbeşyüz) adet uygulama yer almalıdır.

1.2.3. Sistemin uygulama kütüphanesinde en az 18 (onsekiz) farklı uygulama kategorisi tanımlı olmalıdır.

1.2.4. Uygulama kütüphanesinde yer alan tüm uygulamalar aşağıda belirtilen parametrelere göre kategorize edilmiş olmalıdır.

a. Uygulama davranışına göre (botnet, tünelleme amaçlı, bulut uygulaması, bandwith tüketim odaklı, sızma amaçlı),

b. Risk seviyesine göre (Critical, High, Medium, Low, Informational)

c. Dünyadaki kullanım yoğunluğu, popülerlik seviyesine göre,

d. Kullanılan protokole göre (HTTP, DNS, FTP, SIP, H323 gibi)

e. Üreticiye göre (Google, Microsoft, Apple gibi)

f. Erişim yöntemine göre (Client-server, browser tabanlı, P2P gibi)

1.2.5. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir, sistem yöneticileri tarafında istenirse manuel olarak da güncellenebilir olmalıdır.

1.2.6. stenmeyen uygulamaları kullandığı tespit edilen ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

1.2.7. Karantinaya alınan kullanıcılara web arayüzü üzerinden özelleştirilmiş karantina uyarısı çıkarılabilmelidir.

1.2.8. Uygulama kontrol veritabanında yer alan tüm uygulamaların listesi, hangi kategoride yer aldıkları ve risk seviyesi bilgisine üreticinin resmi web sitesi üzerinden erişilebilmeli bu bilgiler herkese açık şekilde yayınlanmış olmalıdır.

1.2.9. Uygulamalar tarafından yapılabilecek DNS trafikleri engellenebilmelidir.

1.2.10. Sistem yöneticileri tarafından özel uygulama imzaları tanımlamaya izin vermelidir.

1.3. IPSec VPN

1.3.1. Sistemin IPSec VPN desteği olmalıdır. DES, 3DES, AES-128, AES-192, AES-256 kriptolama ile MD5, SHA-1, SHA-384, SHA-512 authentication standartlarını desteklemelidir.

1.3.2. Cihazın desteklediği IPSEC tünel sayısı datasheet'lerde belirtilmiş olmalıdır.

1.3.3. Sistem IPSEC tünel içerisinden multicast trafik aktarımına izin vermelidir.

1.3.4. Sistemin VPN Overlay Controller (OCVPN) özelliği olmalıdır. Bu sayede birden fazla güvenlik duvarının bulut ortamı üzerinden otomatik VPN yapması sağlanabilmeli, tüm sistemlerin VPN konfigürasyonlarının bulut üzerinden otomatik olarak senkronize edilmesi desteklenmelidir.

1.4. Bant Genişliği Yönetimi (QoS)

1.4.1. Cihazın detayları aşağıda anlatılan bant genişliği yönetim özelliği olmalıdır.

1.4.2. Kaynak ip/ağ, kullanıcı/kullanıcı grubu, hedef ip/ağ , servis ve uygulama/uygulama kategorisi bazında bant genişliği politikası yazılabilmelidir.

1.4.3. Spesifik uygulama (örneğin Youtube) ve uygulama kategorisi (örneğin Update) bazında bant genişliği politikası yazılabilmelidir.

1.4.4. Erişilen URL kategorisi (örneğin 'Stremaing Media') bazında bant genişliği politikası yazılabilmelidir.

1.4.5. Zaman aralığı bazında bant genişliği politikası yazılabilmelidir (örneğin mesai saatleri içerisinde gibi...).

1.4.6. Birden fazla hat olması durumunda çıkış interface'i bazında bant genişliği politikası yazılabilmelidir. Her bir çıkış interface'i için farklı bant genişliği politikası yazmaya izin vermelidir.

1.4.7. Aynı session içerisinde trafiğin yönüne göre (IN ve OUT yönünde) bant genişliği politikası yazılabilmelidir.

1.4.8. Sistemdeki tüm kullanıcılar için tanımlı bant genişliği kuralı içerisinde ip başına limitasyon yapılabilmelidir. (örneğin tüm kullanıcıları 10 mbps ile limitle gibi..)

1.4.9. Kural bazında bant genişliği politikası yazılabilmelidir. Böylece ilgili kuralla eşleşen trafiklerin limitlenmesi sağlanabilmelidir.

1.4.10. Interface bazında trafiğin yönüne göre (IN ve OUT yönünde) bant genişliği sınırlandırması yapılabilmelidir.

1.5. Saldırı Tespit ve Engelleme (IPS)

1.5.1. Sistemin güncel saldırıların engellenmesi amacıyla aşağıda detayları belirtilen atak engelleme (IPS) özelliği olmalıdır.

1.5.2. IPS sistemi aşağıda belirtilen saldırı tiplerini engelleyebilmelidir.

a. Trafik Anomaly

b. Protocol Anomaly

c. Oran (rate) bazlı saldırılar (brute force gibi)

d. Sızma temelli (evasive) saldırılar

e. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak da yapılabilmelidir.

1.5.3. Her bir IPS imzası için aşağıdaki aksiyonlar alınabilmelidir.

a. İzin ver (pass)

b. İzin ver ve olay kaydı al (monitor)

c. Paketi düşür (block)

d. Paketi düşür ve session'ı sonlandır (Reset)

e. Saldırıyı yapanı karantinaya al

1.5.4. Tanımlı saldırı tiplerine göre saldırı yapan ip adresleri süreli veya süresiz olarak karantinaya alınabilmelidir. Karantinaya alınan adresler sistem yöneticileri tarafından karantina süresinin sonunu beklemeden karantinadan çıkarılabilmelidir.

1.5.5. Veritabanında yer alan imzalar aşağıdaki tanımlara göre filtrelenebilmelidir.

a. Kullanılan uygulamaya göre (IIS, Oracle, SQL, Apache gibi)

b. İşletim sistemine göre (Windows, Linux, Solaris gibi)

c. Protokole göre (HTTP, HTTPS, FTP, DNS gibi)

d. Risk seviyesine göre (Kritik, Yüksek Risk, Orta Risk, Düşük Risk gibi)

e. Hedef işletim sistemine göre (client ve/veya server)

1.5.6. Rate tabanlı saldırı tanımları içerisinde ne kadar sürede kaç adet istekte bulunulabileceği tanımlanabilmelidir. Örneğin OWA'ya 5 sn içerisinde 3'ten fazla login isteğinde bulunulmasın gibi.

1.5.7. IPS sistemi aşağıda belirtilen detaylı sızma tekniklerine karşı koruma sağlayabilmelidir.

a. IP Packet Fragmentation,

b. TCP Stream Fragmentation

c. TCP Stream Segmentation,

d. RPC Fragmentation,

e. URL & HTML Obfuscation,

1.5.8. IPS sistemi Botnet aktivitelerini tespit edebilmeli ve engelleyebilmelidir.

1.5.9. IPS imzası özelinde kaynak ve hedef adres bilgisine dayalı istisna adresler (exception) tanımlanabilmelidir.

1.5.10. IPS sistemi Botnet C&C adreslerine doğru yapılan tüm trafikleri adres tabanlı tespit edebilmeli ve engelleyebilmelidir.

1.5.11. Sistem IPS loglarında saldırının yönünü gösterebilmelidir (client to server veya server to client)

1.6. Yeni Nesil Güvenlik Duvarı (NGFW Firewall)

1.6.1. Cihazın detayları aşağıda belirtilen sanal güvenlik duvarı özelliği olmalıdır:

1.6.2. Cihaz üzerinden birbirinden izole sanal güvenlik duvarları oluşturulabilmelidir.

1.6.3. Cihaz üzerindeki arayüzler veya sanal arayüzler (vlan) sanal güvenlik duvarları arasında paylaştırılabilmelidir.

1.6.4. Her bir sanal güvenlik duvarı için dedike bir sistem yöneticisi atanabilmeli, sistem yöneticilerinin yetkileri olmayan sanal güvenlik duvarlarına erişimleri engellenebilmelidir.

1.6.5. Sanal güvenlik duvarı oluşturulması işlemi web arayüzünden kolayca yapılabilmeli ve çalışan mevcut sistemin reboot edilmesine ihtiyaç olmamalıdır.

1.6.6. Her bir sanal güvenlik duvarı üzerinde açılabilecek maksiumum oturum (session) sayısı limitlenebilmelidir.

1.6.7. Önerilecek çözüm, güncel “Gartner Magic Quadrant Enterprise Network Firewalls” raporunda “Leaders” kategorisinde yer almalıdır.

1.7. DOS Engelleme

1.7.1. Cihazın detayları aşağıda belirtilen servis dışı bırakma saldırılarını (DoS) engelleme özelliği olmalıdır.

1.7.2. DoS politikaları ile internetten erişilebilir sistemlere (web server, dns server gibi) yönelik trafikler için eşik değer (threshold) bazlı sınırlandırma yapılabilmelidir.

1.7.3. L3 seviyesinde kaynak ve hedef ip bazında açılabilecek toplam oturum sayısı (session) limitlenebilmelidir.

1.7.4. L4 seviyesinde TCP, UDP , ICMP ve SCTP protokolleri için kaynak ve hedef ip bazında açılabilecek oturum sayısı limitlenebilmelidir.

1.7.5. Sistem portscan ve udpscan saldırılarını tespit edip engelleyebilmelidir.

1.7.6. TCP synflood ve UDP flood saldırılarına karşı aynı kaynaktan aynı anda gelebilecek syn istek sayısı limitlenebilmelidir.

1.7.7. Sistem IPv6 adresleri için de yukarıda belirtilen anti-DoS özelliklerini desteklemelidir.

1.7.8. Belirtilen tüm DoS politika konfigürasyonları cihazın web arayüzünden yapılabilmelidir.

1.8. Virüs/Zararlı İçerik Kontrolü

1.8.1. Sistem üzerinde detayları aşağıda belirtilen zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır.

1.8.2. Sistem aşağıda belirtilen protokoller aracılığıyla yapılan malware trafiklerini tespit edip engelleyebilmelidir.

a. HTTP(S)
b. FTP(S)
c. POP3(S)
d. IMAP(S)
e. SMTP(S)

1.8.3. Sistem, yukarıda belirtilen protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir.

1.8.4. AntiMalware sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmeli, gerekmesi durumunda antivirüs veritabanı manuel olarak güncellenebilmelidir.

1.8.5. Sadece internet trafiğinde değil, istenirse lokal network erişimlerinde de AntiMalware kontrolü yapılabilmelidir.

1.8.6. AntiMalware sistemi, akıllı telefonlara yönelik mobil malware'leri tespit edebilme ve engelleme yeteneğine sahip olmalıdır.

1.8.7. Arşiv dosyalarının detay analizini yapabilmeli ve bozuk (corrupted), şifreli (encrypted), içiçe geçirilmiş (nested) arşiv dosyaları engellenebilmelidir.

1.8.8. Malware içerdiği tespit edilen kaynak adresler otomatik olarak karantinaya alınabilmelidir.

1.8.9. AntiMalware sistemi dış kaynaklarla otomatik entegrasyon özelliğine sahip olmalı, dış kaynaklardan alınan malware hash (feed) bilgilerine göre kontrol ve engelleme özelliği olmalıdır. Sistem dış kaynaklardan aldığı hash verisini otomatik olarak güncelleyebilmeli ,sistem yöneticilerinin manuel işlem yapmasına ihtiyaç olmamalıdır.

1.8.10. Sistem, yeni yayılım gösteren ve henüz imza güncellemesi olmayan virüslere karşı gerçek zamanlı istihbarat servis sorgulaması yapabilmelidir. Böylece yeni ortaya çıkmış ancak lokal veritabanında yer almayan virüs saldırılarına karşı koruma sağlayabilmelidir.

1.8.11. Sistem, içerisinde zararlı potansiyeli olan bileşenleri dosya içerisinden çıkararak dosyayı tamamen güvenli bir şekilde kullanıcıya iletme özelliğine sahip olmalıdır. Bu kapsamda en az aşağıda belirtilen objeler dosya içerisinden çıkarılabilmelidir.

a. Gömülü objeler
b. Makrolar
c. Linkler
d. Java kodları
e. Cover page

1.9. URL Filtreleme

1.9.1. Sistem üzerinde detayları aşağıda iletilen URL Filtreleme özelliği bulunmalıdır.

1.9.2. URL filtreleme veritabanında en az 250 milyon web adresi tanımlı olmalıdır.

1.9.3. En az 80 farklı kategori tanımı olmalıdır.

1.9.4. Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk url adresi, regex ve wildcard formatında tanımlı adreslere erişime izin verebilmeli veya engelleme yapabilmelidir.

1.9.5. Site içeriği taraması yapılabilmelidir. Regex ve wildcard formatında belirtilen text'i içeren sitelere erişim engellenebilmeli ya da izin verebilmelidir.

1.9.6. USOM gibi harici karaliste kaynakları spesifik kategori olarak eklenebilmeli ve otomatik olarak güncellenebilmelidir.

1.9.7. Sadece domain bazında değil, erişilen ip bazında da kontrol yapabilmelidir.

1.9.8. URL bloklama ekranı özelleştirilebilmelidir.

1.9.9. Farklı kullanıcı ve kullanıcı gruplarına farklı URL filtreleme profilleri uygulanabilmelidir.

1.9.10. URL filtreleme lokal cache timeout süresi sistem yöneticileri tarafından ayarlanabilir olmalıdır.

1.10. DNS Filtreleme

1.10.1. Sistem üzerinde detayları aşağıda belirtilen DNS Filtreleme özelliği bulunmalıdır.

1.10.2. Lokal veya internet DNS sunucularına doğru yapılan DNS sorguları kontrol edilerek istenmeyen adresler için yapılan sorgulara sistem yöneticileri tarafından belirlenen ip adresinin döndürülmesi sağlanabilmelidir.

1.10.3. URL filtreleme veritabanı aynı zamanda DNS filtreleme amacıyla da kullanılabilmelidir.

1.10.4. Karaliste ve beyazliste özelliği olmalıdır. Bu sayede direk domain adresi, regex ve wildcard formatında tanımlı adreslere DNS sorgusu yapılmasına izin verebilmeli ya da bloklama yapabilmelidir.

1.10.5. USOM gibi harici karaliste kaynakları spesifik DNS kategorisi olarak eklenebilmeli ve otomatik olarak güncellenebilmelidir. Bu listede yer alan domain adreslerine yapılan DNS sorgularında sistem yöneticileri tarafından belirlenen ip adresinin döndürülmesi sağlanabilmelidir.

1.10.6. Kurumun internetten sorgulara açık olan DNS sunucularına doğru sadece kurum domain'i için yapılan DNS sorgulamalarına izin verilmesi, diğer tüm alan adları için yapılan DNS isteklerinin bloklanması sağlanabilmelidir.

1.10.7. Sistemin DNS translation özelliği olmalıdır.

1.11. SSL VPN

1.11.1. Kurum kaynaklarına uzaktan güvenli erişiminin sağlanabilmesi için cihaz üzerinde aşağıda detayları belirtilen SSL-VPN özelliği olmalıdır.

1.11.2. SSL VPN istemcisi en az aşağıdaki işletim sistemlerini desteklemelidir.

a. Windows
b. Mac OS
c. Linux
d. IOS
e. Android
f. Chromebook

1.11.3. Web portal üzerinden herhangi bir yazılım yüklemeden (agentless) SSL VPN bağlantısını desteklemelidir.

1.11.4. Web portal üzerinden bağlantılarda aşağıdaki uygulamaları çalıştırabilmelidir.

a. Web erişimleri (HTTP/HTTPS)
b. RDP
c. SSH/TELNET
d. FTP
e. SMB/CIFS dosya paylaşımları

1.11.5. Farklı kullanıcılar için farklı web portallerini desteklemelidir.

1.11.6. Farklı kullanıcılara farklı ip adresleri atanmasını desteklemelidir.

1.11.7. SSL VPN üzerinden erişen kullanıcıların lokal kullanıcı veritabanı, RADIUS, LDAP veya Microsoft AD üzerinden kimlikleri doğrulanabilmelidir.

1.11.8. SSL VPN tüneli içerisinden gelen trafiklerde IPS, Uygulama Kontrolü, AntiMalware, URL Filtreleme özellikleri uygulanabilir olmalıdır.

1.11.9. DNS server için split tunneling'i desteklemelidir. Bu sayede sadece spesifik domain sorguları için merkezdeki DNS sunucularının kullanımı sağlanabilmelidir.

1.11.10. SSL-VPN ile bağlantı yapacak adresler belirtilebilmeli, belirtilen adresler dışından SSL-VPN erişimleri engellenebilmelidir.

1.11.11. Split tunelling özelliği ile sadece belirtilen hedef adresler için trafiğin tünele yönlendirilmesi sağlanabilmelidir.

1.11.12. SSL-VPN ile bağlanacak kullanıcılar için two factor authentication (2FA) özelliği desteklenmelidir.

1.11.13. SSL-VPN ile yapılan aktif bağlantılar monitör edilmelidir. Bağlı olan kullanıcı ve ne zaman login olduğu bilgilerine web arayüzü üzerinden erişilebilmelidir.

1.12. GENEL ÖZELLİKLER

1.12.1. Network arayüzlerinin herbiri LAN, WAN, DMZ veya kullanıcı tanımlı bir segment olarak konfigüre edilebilmelidir. İlgili arayüzler 802.1q protokolünü desteklemelidir. Her bir interface için Alias tanımı girilebilmelidir.

1.12.2. Yönetim arayüzü üzerinden her bir fiziksel, sanal interface ve interface grubuna ait (LACP) trafik kullanım değerleri gerçek zamanlı ve geçmişe dönük görüntülenebilmelidir. Bu sayede hangi interface üzerinde ne kadar trafik kullanımı olduğu bilgisi (throughput) IN ve OUT yönlü analiz edilebilmelidir.

1.12.3. Sistemin SPI (Stateful Packet Inspection) özelliği olmalıdır.

1.12.4. Sistem BGP, OSPF ve RIP dinamik routing protokolleri aracılığıyla ADVPN özelliğini desteklemelidir. Bu sayede merkez lokasyonla VPN yapan bölgeler kendi aralarında otomatik bağlantı kurabilmelidir.

1.12.5. Multicast routing'i desteklemelidir.

1.12.6. İstenirse source nat işlemi esnasında source portun nat'lanmaması (preserve soruce port) özelliği desteklenmelidir.

1.12.7. Sistem, HTTP/2 protokolünü desteklemeli, HTTP/2 protokolü kullanılarak yapılan trafiği tespit edebilmelidir.

1.12.8. DHCP Server ve DHCP Relay özelliği bulunmalıdır. Uç noktada açılan Vlan'lar için DHCP'den ip dağıtabilmeli ya da relay yapabilmelidir.

1.12.9. Sistem, routing tablosuna bakarak spoof saldırılarını tespit edebilmelidir.

1.12.10. Cihaz üzerinde 'rota arama' (route searching) özelliği olmalıdır. Bu sayede spesifik bir adres için trafiğin hangi rota (route) üzerinden gideceği web arayüzü üzerinden kolaylıkla tespit edilebilmelidir.

1.12.11. NAT64 ve Jumbo frame desteği olmalıdır.

1.12.12. Ağ arayüzü veya zone bazlı kural yazılmasını desteklemelidir. Tüm kurallar trafiğin yönüne göre giriş ve çıkış interface'i bazında (interface pair) otomatik gruplandırılabilmelidir.

1.12.13. Saat, gün, tarih bazında güvenlik erişim kontrolü yapabilmelidir.

1.12.14. MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılmasına olanak tanımalı, tutulan kayıtlarda kullanıcı ismi yer alabilmelidir. Bu sayede trafiği yaratan kaynağın isim ile takibinin yapılabilmesine olanak sağlamalıdır.

1.12.15. Kullanıcıları ve kullanıcı gruplarını otomatik olarak Active Directory'den okuyabilmelidir.

1.12.16. Kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS, LDAP ve AD üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

1.12.17. Sistem yöneticilerinin otomatik üretilen tek seferlik şifre (OTP) ile cihaza bağlantı yapmasını desteklemelidir. Bu özellik en az iki sistem yöneticisi için desteklenmeli, sistem yöneticilerinin akıllı telefonlarına yüklenen uygulama ile tek seferlik şifre üretimi sağlanabilmelidir.

1.12.18. Inbounda ve outbound SSL inspection özelliği olmalıdır. TLS v1.3 trafiği üzerinde SSL Inspection yapabilmeldir.

1.12.19. Cihaz üzerinde sertifika blacklisting özelliği olmalıdır. Bu sayede güvenilir olmayan sertifika kullanan sistemlerle bağlantılar engellenebilmelidir. Blacklisted sertifika veritabanı sistem tarafından otomatik olarak güncellenecektir.

1.12.20. MAC adres aralığı bazında kural yazımını desteklemelidir.

1.12.21. Teklif edilen sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama, Ping6, IPv6 captive portal, IPv6 FQDN adresleri desteklenmelidir.

1.12.22. SNMPv3'ü desteklemelidir.

1.12.23. Sistem, ani elektrik kesintileri gibi durumlarda yeniden başlatıldıklarında sistem yöneticilerinin manuel müdahalesi olmaksızın otomatik dosya sistemi kontrolü yapabilmelidir.

1.12.24. Sistemin harici kara listeler üzerinden otomatik olarak çektiği ip adreslerine doğru yapılan trafikler veya bu adrelerden kuruma yapılan trafikler kural bazında engellenebilmelidir.

1.12.25. İşletim sistemi ve yazılım güncellemeleri web ara yüzü üzerinden yapılabilmelidir. Yedekli (cluster) çalışan sistemlerin güncellemeleri aktif cihaz aracılığıyla otomatik olarak yapılmalı, iki cihaz üzerinde ayrı ayrı manuel güncellemeye ihtiyaç olmamalıdır.

1.12.26. Birden fazla internet hattının olması durumunda yukarıda belirtilen internet servis veritabanı kullanılarak spesifik üretici ve uygulama trafiklerinin belirtilen internet hattı üzerinden yönlendirilmesi sağlanabilmelidir. Örneğin Amazon, Dropbox, Facebook sunucularına giden trafiği A hattından, diğer trafikleri B hattından yönlendir gibi.

1.12.27. Yedekli yapıda (cluster) çalışan sistemler üzerinde sanal güvenlik duvarları tercihe bağlı olarak aktif-pasif şekilde dağıtılabilmeli ve sanal güvenlik duvarı seviyesinde yük paylaşımı yapılabilmelidir.

1.12.28. Sistemin session senkronizasyon özelliği olmalıdır. Bu özellik sayesinde load balancer veya router gibi trafik dağıtımı yapan cihazlar arkasında çalışan birbirinden bağımsız (cluster olmayan) sistemler kendi aralarında session senkronizasyonu yapabilmeli, cihazlardan birisinin arızalandığı durumda load balancer tarafından tüm trafik öteki cihaza aktarıldığında da mevcut session'ların devamlılığı sağlanabilmelidir.

1.12.29. İşletim sistemi ve yazılım güncellemelerini web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

1.12.30. Sistemin 'Tehdit Haritalama' özeliği olmalıdır. Bu sayede cihazın bulunduğu coğrafi bölgeye gelen saldırılar dünya haritası üzerinden saldırıların yapıldığı kaynak ülke bilgisini de içerecek şekilde gerçek zamanlı (anlık) olarak görülebilmelidir.

1.12.31. Cihazın yönetim arayüzü üzerinden sistemle ilgili aşağıdaki detay bilgilere ulaşılabilmelidir.

a. Seri no, Firmware versiyonu ve Uptime bilgisi,

b. Saniyede oluşan bağlantı isteği sayısı (connection per second),

c. Mevcut oturum (session) sayısı,

d. CPU, Memory değeri (yüzdesel),

e. Lisans durumu,

f. WAN interface'inin ip adresi ve karalisteye alınmış ise bilgisi,

g. Sisteme bağlı olan admin'lerin bilgisi,

1.12.32. Sistemin konfigürasyon ve 'Best Practise' kontrol özelliği olmalıdır. Bu sayede cihazın konfigürasyon denetimini yapabilmeli ve konfigürasyon eksikliklerliyle ilgili (örneğin interface'ler üzerinden güvenli olmayan web servis erişiminin açık olması, admin şifrelerinin standartlara uygun olmaması gibi) önerilerde bulunabilmelidir. Bu sayede sistemin güvenlik düzeyi arttırılmalıdır.

1.12.33. Cihazın interface ve adres objeleri oluşturulurken etiketleme (tagging) özelliği olmalıdır. Bu sayede obje oluşturulurken önceden tanımlanmış zorunlu etiketlerden en az birinin seçilmesi desteklenmelidir. Örneğin adres objesini oluştururken hangi admin'in bu objeyi oluşturduğunun bilinmesi için önceden tanımlanmış admin etiketlerinden (örneğin isimlerinden) birisinin zorunlu olarak seçilmesi, seçilmemesi durumunda ise objenin oluşturulmaması sağlanmalıdır.

1.12.34. Cihazın proaktif mimaride otomatik aksiyon alabilme özelliği olmalıdır. Bu özellik sayesinde aşağıdaki olaylardan birisi gerçekleştiğinde otomatik olarak eposta gönderimi, register edilmiş olan IPhone'a push notifikasyon gönderimi ve herhangi bir web servisini tetikleme aksiyonlarını otomatik olarak alabilmelidir.

a. Konfigürasyon değişikliği yapıldığında,

b. Cihaz kapanıp açıldığında olduğunda,

c. Lisans süresi bittiğinde,

d. Yedekli (cluster) cihazlar arasında geçiş yaşandığında,

e. AV veya IPS database'i güncellendiğinde,

f. Sistemde önceden tanımlı herhangi bir olay gerçekleştiğinde (örneğin güncelleme işlemi başarısız olduğunda, AD entegrasyonunda sorun olduğunda, IPSec bağlantısı düştüğünde gibi..)

g. Aynı üreticinin ait korelasyon ve raporlama ürünü üzerinde sistem yöneticileri tarafından tanımlanan bir olay gerçekleştiğinde (örneğin database sunucusuna üç kere arka arkaya hatalı şifre girilmesi gibi)

h. Tanımlanmış zaman aralıklarına göre (örneğin hergün saat 23:00'de yapılması istenen bir işlem olduğunda)

1.12.35. Yukardaki maddede belirtilen olaylardan birisi gerçekleştiğinden sistem otomatik olarak aşağıdaki aksiyonları alabilmelidir.

a. Otomatik olarak eposta gönderimi,

b. Register edilmiş olan IPhone'a push notifikasyon gönderimi
c. Lokalde çalışan bir web servisini çağırma,
d. Otomatik script çalıştırma
e. Amazon Web servisini çağırma
f. Microsoft Azure üzerinden bir servisi çağırma
g. Google Cloud platromu üzerinden bir servisi çağırma
h. AliBaba Cloud platformu üzerinden bir servisi çağırma

1.12.36. Cihazın aşağıda belirtilen SDN (private cloud) ve bulut (public cloud) temelli çözümlerle API entegrasyonu olmalıdır. Entegrasyon yapılan ürünlere ait tanımlanan dinamik objeler bazında güvenlik politikaları tanımlanabilmelidir.

a. Cisco ACI
b. Amazon Web Service
c. Microsoft Azure
d. VMware NSX
e. VMware ESXi
f. Nuage Virtulized Service Platform
g. Oracle OCI
h. OpenStack (Horizon)
i. Google Cloud Platform (GCP)
j. AliBaba Cloud
k. Kubernetes

1.12.37. Cihaz üzerinde çok kullanılan sistem, ağ ve güvenlik üreticilerinin hizmet amaçlı kullandıkları Web, DNS, FTP v.b. sunucularının ip ve servis bilgilerinin yer aldığı internet servis veritabanı olmalıdır. Bu sayede üreticilerin hizmet verdiği sunuculara erişimler için veritabanında yer alan objeler kolayca seçilebilmeli, örneğin Microsoft sunucularına veya güncelleme için antivirüs üreticilerine doğru erişim izin kuralı yazılabilmelidir. Internet servis veritabanı sistem tarafından otomatik olarak güncellenmelidir. Internet servis veritabanı içerisinde herhangi bir üreticiye ait ip erişimlerinin hangi portlar üzerinden yapılabileceği sistem yöneticileri tarafından istenirse manuel olarak tanımlanabilmelidir.

2. SD-WAN Ürünü Performans ve Donanım Özellikleri (Şubeler Veri Hızı 50 Mbit/s ile 200 Mbit/s arası) – (3 adet)

2.1. Teklif edilen sistem, teklif edilen konfigürasyonda, en az 20 Gbps Firewall performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

2.2. Ürün, en az 2 Gbps uygulama kontrol (application control) performans (throughput) değerine sahip olmalıdır. Bu değer RFC standartlarında ölçülmüş lab değeri olmamalı, gerçek yaşam (Enterprise Mix) değeri olmalıdır.

2.3. Ürün, en az 1,5 Gbps yeni nesil firewall (Firewall, Uygulama Kontrol ve IPS servisleri aktif) performans (throughput) değerine sahip olmalıdır. Bu değer RFC standartlarında ölçülmüş lab değeri olmamalı, gerçek yaşam (Enterprise Mix) değeri olmalıdır.

2.4. Ürün en az 2,5 Gbps saldırı engelleme (IPS) performans (throughput) değerine sahip olmalıdır. Bu değer RFC standartlarında ölçülmüş lab değeri olmamalı, gerçek yaşam (Enterprise Mix) değeri olmalıdır.

2.5. SSL Inspection aktif olduğu durumda cihazın HTTPS paketleri için IPS performans değeri en az 1 Gbps olmalıdır.

2.6. Ürün en az 10 Gpbs IPSEC VPN performans değerine sahip olmalıdır.

2.7. Ürün, aynı anda en az 1.3 milyon oturumu desteklemelidir.

2.8. Ürün, saniyede en az 50.000 yeni oturum açabilme kapasitesine sahip olmalıdır.

2.9. Ürün, aynı anda en az 18 adet GE bakır port bulundurmalıdır.

2.10. Ürün, aynı anda en az 2 adet 10Gbit SFP+ ve 8 Adet SFP port bulundurmalıdır.

2.11. Cihaz aynı anda 200 kullanıcının SSL VPN ile bağlantısına izin verebilecek kapasitede olmalıdır.

2.12. Cihaz üzerinde aynı anda 10 adet sanal güvenlik duvarı oluşturulabilmelidir. Gerekmesi durumunda ilgili lisanslar teklife dahil edilecektir.

2.13. Kurum, üreticinin resmi web sayfasında yayınlanan datasheet değerlerinin doğruluğunu kontrol amacıyla bağımsız test kuruluşlarının (NSS Labs v.b.) yaptığı ve ilgili üreticinin en az bir ürününe ait performans testinin sonuçlarını talep etme hakkına sahiptir.

2.14. Sistemin; Firewall, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.