TÜRK HAVA KURUMU ÜNİVERSİTESİ

BİRLEŞİK TEHDİT YÖNETİMİ CİHAZI, KAYIT SİSTEMİ VE KİMLİK DOĞRULAMA SİSTEMİ TEKNİK ŞARTNAMESİ

1. KAPSAM

1.1. Bu şartname; Türk Hava Kurumu Üniversitesi ve bağlı olan birimlerde siber güvenliğin temin edilebilmesi amacıyla bu şartname kapsamında tanımlanan güvenlik hizmetlerinin karşılanabilmesine yönelik olarak mevcutta bulunan cihazların lisanslarının uzatılması için lisans tedariki veya mevcutların yerine yeni cihaz ve lisans tedarikini kapsamaktadır.

2. GENEL ŞARTLAR

2.1. Türk Hava Kurumu Üniversitesi Etimesgut/Ankara'da Türkkuşu Kampüsü, Akköprü/Ankara'da Akköprü Kampüsü ve Selçuk/İzmir'de Selçuk Kampüsü ile eğitim/öğretim hizmeti vermektedir.

2.2. Her kampüsün ayrı bir internet bağlantısı olup, kampüsler arasında birleşik tehdit yönetimi cihazları üzerinden VPN bağlantısı kullanılmaktadır. Kampüslerin halihazırda internet bağlantı hızları şu şekildedir:

Türkkuşu Kampüsü: 170 Mbps

Akköprü Kampüsü: 40 Mbps (Uzaktan eğitim dönemlerinde 100 Mbps)

Selçuk Kampüsü: 20 Mbps

2.3. Kampüslerdeki personel ve öğrenci mevcudu şu şekildedir:

Türkkuşu Kampüsü: 3000

Akköprü Kampüsü: 800

Selçuk Kampüsü: 300

2.4. Kampüslerimizde halen kullanılmakta olan cihaz marka ve modelleri şu şekildedir:
Türkkuşu Kampüsü: Sophos XG-450

Akköprü Kampüsü: Sophos XG-210

Selçuk Kampüsü: Sophos XG-210

2.5. Tip-1 cihaz Türkkuşu Kampüsünde, Tip-2 cihazlar Akköprü ve Selçuk Kampüs'lerinde hizmet verecek şekilde yapılandırılacaktır.

2.6. İstekliler ya mevcut cihazların lisanslarını bu şartnamede tanımlanan isterlere göre 36 (otuzaltı) ay süreli olarak uzatacak veya alternatif olarak bu şartnamede tanımlanan isterlere uygun yeni cihaz ve lisans verilecek şekilde teklif sunacaklardır.

2.7. İhale kapsamında yer alan tüm donanım ve yazılımların İdareye teslimini müteakip, İDARE'ce gösterilecek yerlere, eski cihazlardaki yapılandırma ile ve mevcut sistemle entegre olacak şekilde kurulumu yapılacak ve tüm sistem çalışır durumda teslim edilecektir.

3. TEKNİK ÖZELLİKLER

3.1. BİRLEŞİK TEHDİT CİHAZI TİP-1

3.1.1. Güvenlik duvarı çözümleri bu iş için özel olarak üretilmiş bir donanım ve yazılım bütünü (appliance) olarak teklif edilecektir.

3.1.2. Teklif edilecek güvenlik duvarı çözümleri ve yönetim modülü aynı üreticiye ait olmalıdır.

3.1.3. Güvenlik duvarı ürünlerinin en az 3.5 (üçnoktabeş) Gbps (Next Generation Firewall throughput kapasitesine sahip olacaktır.

3.1.4. Güvenlik duvarı en az 2 (iki) Gbps Next Generation Threat Prevention throughput değerine sahip olacaktır.

3.1.5. Güvenlik duvarı en az 4 (dört) Gbps VPN throughput değerine sahip olacaktır.

3.1.6. Güvenlik duvarı ürünleri, 1.5 (birnoktabeş) Milyon adet eş zamanlı oturumu (concurrent session) desteklemelidir.

3.1.7. Güvenlik duvarı ürünleri, 25.000 (yirmibeşbin)adet anlık bağlantı isteğini (connection per second) karşılayabilmelidir.

3.1.8. Güvenlik duvarı ürünleri üzerinde en az 240 (ikiyüzkırk) GB kapasiteli SSD disk bulunmalıdır.

3.1.9. Güvenlik duvarı ürünlerinin üzerinde en az 6 (altı) adet 10/100/1000 Mbps bakır bağlantı ethernet ağ arayüzü ve en az 2 (iki) adet Gigabit Ethernet SFP arayüzü bulunmalıdır.

3.1.10. Teklif edilen güvenlik ürünü, aynı donanım üzerinde NGFW (Next Generation Firewall) ve VPN fonksiyonlarını çalıştırabilecektir.

3.1.11. Teklif edilen güvenlik ürünü içerik filtreleme ve anti-virus devrede iken Aktif/Pasif yedekli çalışmayı destekleyecektir.

3.1.12. Güvenlik duvarı ürünleri, mimari açıdan stateful inspection ve IP paket filtreleme özelliklerini bünyesinde bulundurmalıdır.

3.1.13. MS Active Directory ile entegre olarak kişi, grup bazında firewall kuralı yazılmasına olanak tanımalı, tutulan kayıtlarda kullanıcı ismine olanak sağlayacaktır.

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

3.1.15. İnternette kullanılan TCP, UDP ve ICMP tabanlı protokolleri desteklemelidir. Kullanıcı tanımlı servis hizmeti tanımlamaya izin vermelidir.

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

3.1.17. 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.

3.1.18. Port adres çevrim (PAT) özelliğine sahip olmalıdır.

3.1.19. Layer2 ve Layer3 ağlarda client cihaz mac adreslerini loglara düşürebilmelidir.

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

3.1.21. Site to site ve client to site VPN desteği olmalıdır.

3.1.22. Güvenlik duvarı, IPSec VPN standardını desteklemelidir.

3.1.23. Cihazın IPS özelliği olmalıdır.

3.1.24. Farklı ülkelerden gelebilecek trafiği tehdit anında kesebilmelidir. Coğrafi koruma sağlayabilmelidir.

3.1.25. IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza kategorisi için ayrı ayrı ayarlanabilmelidir.

3.1.26. 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.

3.1.27. IPS fonksiyonu aşağıdaki saldırı tiplerine karşı koyabilmelidir;

3.1.27.1. Backdoors

3.1.27.2. Botnets

3.1.27.3. Denial of Service (DoS)

3.1.27.4. Anlık mesajlaşma (Skype, vb.)

3.1.27.5. İşletim sistemlerine dönük saldırılar

3.1.27.6. Peer-to-peer (BitTorrent, Ares, vb.)

3.1.27.7. Protocol tunneling

3.1.27.8. Traffic Anomaly

3.1.27.9. Protocol Anomaly

3.1.28. SNI (Server Name Indication) üzerinden HTTPS trafiğini filtreleyebilme ve loglama özelliği olmalıdır.

3.1.29. Güvenlik duvarı, IPS, Uygulama Kontrolü, URL Filtreleme ve Anti Virüs kontrollerini uygulayabilmelidir.

3.1.30. SNI üzerinden HTTPS trafiğinin incelenmesi için erişim rolü, bilgisayar/sunucu, ağ bazında kural yazılabilmelidir.

3.1.31. Cihaz üzerinde en az 500 (beşyüz) adet uygulamayı tanıyabilen uygulama kontrolü özelliği olacaktır.

3.1.32. Uygulama kontrolü özelliği active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve gruplar bazında uygulama kontrolü kuralları tanımlanabilecektir.

3.1.33. Cihaz üzerinde içerik filtreleme (URL filtreleme) özelliği olacaktır. URL filtreleme özelliği en az 50 (elli) farklı kategori ve en az 90 (doksan) milyon URL adresini kategorize etme özelliğine sahip olmalıdır.

3.1.34. İçerik filtreleme özelliği, active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı, bilgisayar ve gruplar bazında içerik filtreleme kuralları tanımlanabilecektir.

3.1.35. Bloklama ekranı olacak ve Türkçe desteği olacaktır.

3.1.36. Antivirüs tarayıcısı olarak çalışabilmeli, SMTP, POP3, HTTP trafiğini virüse karşı tarayabilmeli, tarama işlemini her protokol için trafiğin yönüne veya kaynak/hedef adrese göre yapabilmelidir.

3.1.37. Güvenlik duvarının Anti Virüs özelliği olmalıdır.

3.1.38. SMTP, POP3, HTTP trafiğini virüse karşı tarayabilmeli, tarama işlemini her protokol için trafiğin yönüne ve kaynak/hedef adrese göre yapabilmelidir.

3.1.39. Bilinen virüsler için imza temelli bloklama yapabilmelidir.

3.1.40. 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.

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

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

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

3.1.41.3. Bilinen botnet'ler için imza temelli bloklama yapabilmelidir

3.2. BİRLEŞİK TEHDİT CİHAZI TİP-2

3.2.1. Güvenlik duvarı çözümleri donanım ve yazılım bütünü (appliance) olarak teklif edilecektir.

3.2.2. Teklif edilecek güvenlik duvarı çözümleri ve yönetim modülü aynı üreticiye ait olmalıdır.

3.2.3. Güvenlik duvarı ürünlerinin en az 1 (bir) (Gbps Next Generation Firewall throughput kapasitesine sahip olacaktır.

3.2.4. Güvenlik duvarı en az 0.9 (sıfırnoktadokuz) Gbps Next Generation Threat Prevention throughput değerine sahip olacaktır.

3.2.5. Güvenlik duvarı en az 1.5 (birnoktabeş) Gbps VPN throughput değerine sahip olacaktır.

3.2.6. Güvenlik duvarı ürünleri, en az 500.000 (beşyüzbin) adet eş zamanlı oturumu (concurrent session) desteklemelidir.

3.2.7. Güvenlik duvarı ürünleri, en az 10.000 (onbin) adet anlık bağlantı isteğini (connection per second) karşılayabilmelidir.

3.2.8. Güvenlik duvarı ürünleri üzerinde en az 32 (otuziki) GB depolama alanı bulunmalıdır.

3.2.9. Güvenlik duvarı ürünlerinin üzerinde en az 6 (altı) adet 10/100/1000 Mbps bakır bağlantı ethernet ağ arayüzü bulunmalıdır.

3.2.10. Teklif edilen güvenlik ürünü, aynı donanım üzerinde NGFW (Next Generation Firewall) ve VPN fonksiyonlarını çalıştırabilecektir.

3.2.11. Teklif edilen güvenlik ürünü içerik filtreleme ve anti-virus devrede iken Aktif/Pasif yedekli çalışmayı destekleyecektir.

3.2.12. Güvenlik duvarı ürünleri, mimari açıdan stateful inspection ve IP paket filtreleme özelliklerini bünyesinde bulundurmalıdır.

3.2.13. MS Active Directory ile entegre olarak kişi, grup bazında firewall kuralı yazılmasına olanak tanımalı, tutulan kayıtlarda kullanıcı ismine olanak sağlayacaktır.

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

3.2.15. İnternette kullanılan TCP, UDP ve ICMP tabanlı protokolleri desteklemelidir. Kullanıcı tanımlı servis hizmeti tanımlamaya izin vermelidir.

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

3.2.17. 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.

3.2.18. Port adres çevrim (PAT) özelliğine sahip olmalıdır.

3.2.19. Layer2 ve Layer3 ağlarda client cihaz mac adreslerini loglara düşürebilmelidir.

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

3.2.21. Site to site ve client to site VPN desteği olmalıdır.

3.2.22. Güvenlik duvarı, IPSec VPN standardını desteklemelidir.

3.2.23. Cihazın IPS özelliği olmalıdır.

3.2.24. Farklı ülkelerden gelebilecek trafiği tehdit anında kesebilmelidir. Coğrafi koruma sağlayabilmelidir.

3.2.25. IPS sisteminin saldırıları karşılama biçimi, sistem yöneticisi tarafından her bir imza kategorisi için ayrı ayrı ayarlanabilmelidir.

3.2.26. 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.

3.2.27. SNI (Server Name Indication) üzerinden HTTPS trafiğini filtreleyebilme ve loglama özelliği olmalıdır.

3.2.28. Güvenlik duvarı, IPS, Uygulama Kontrolü, URL Filtreleme ve Anti Virüs kontrollerini uygulayabilmelidir.

3.2.29. SNI üzerinden HTTPS trafiğinin incelenmesi için erişim rolü, bilgisayar/sunucu, ağ bazında kural yazılabilmelidir.

3.2.30. Cihaz üzerinde en az 500 (beşyüz) adet uygulamayı tanıyabilen uygulama kontrolü özelliği olacaktır. Talebe istinaden uygulama imzası oluşturabilmelidir.

3.2.31. Uygulama kontrolü özelliği active directory ile entegre çalışabilecek bu sayede active directory'de tanımlı olan kullanıcı ve gruplar bazında uygulama kontrolü kuralları tanımlanabilecektir.

3.2.32. Antivirüs tarayıcısı olarak çalışabilmeli, SMTP, POP3, HTTP trafiğini virüse karşı tarayabilmeli, tarama işlemini her protokol için trafiğin yönüne veya kaynak/hedef adrese göre yapabilmelidir.

3.2.33. Güvenlik duvarının Anti Virüs özelliği olmalıdır.

3.2.34. SMTP, POP3, HTTP trafiğini virüse karşı tarayabilmeli, tarama işlemini her protokol için trafiğin yönüne ve kaynak/hedef adrese göre yapabilmelidir.

3.2.35. Bilinen virüsler için imza temelli bloklama yapabilmelidir.

3.2.36. Cihaz üzerinde detayları aşağıda verilen botnet tespit ve engelleme özelliği olmalıdır.

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

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

3.2.36.3. Bilinen botnet'ler için imza temelli bloklama yapabilmelidir.

3.3. 5651 SAYILI KANUN UYUMLU KAYIT SİSTEMİ

3.3.1. Önerilen sistem ile birlikte 5651 yasası gerekliliklerini karşılamak için yazılım veya donanım olarak kayıt (loglama) çözümü önerilmelidir.

3.3.2. Teklif edilecek Kayıt Sistemi, teklif edilen cihaz ile bütünleşik veya kurumda mevcut sanal altyapısına kurulabilecek yazılımsal bir çözüm olacaktır.

3.3.3. Sistem yazılım olarak teklif edilirse, Windows işletim sistemleri üzerinde veya Linux sistemleri üzerinde çalışabilmelidir. Sunucu için İdare tarafından sağlanacak sanal sunucu kullanılabilecektir.

3.3.4. Kayıt Sistemi aynı marka en az 2 (iki) adet Güvenlik Sistemine ait log'ları tutabilmeli ve raporlama yapabilmelidir.

3.3.5. Kayıt Sistemi en az 2 (iki) TB disk desteklemelidir.

3.3.6. Sistem tarafından imzalanmış loglar, yedeklemek amacı ile manuel olarak istenilen bir başka depolama alanına kopyalanabilmelidir.

3.3.7. Kayıt Sistemi, log kayıtlarını ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek log yedekliliği sağlayabilmelidir.

3.3.8. Kayıt Sistemi; html, pdf veya benzer doküman formatlarında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine gönderebilmeli ve ftp veya web sitelerine otomatik olarak yükleyebilmelidir.

3.3.9. Sistem 3 (üç) yıllık Güncelleme ve Destek paketi ile birlikte teklif edilmelidir. Sistem ile birlikte 3 (üç) yıl süre ile yazılım güncellemelerini yapacak lisanslar verilmelidir ve servis ve güncellemeleri bu süre boyunca sağlanmalıdır.

3.3.10. Log Kayıtlarında 5651 yasasını belirtmiş olduğu İç IP adres bilgileri, kullanıma başlama ve bitiş tarih ve saati ve bu IP adreslerini kullanan bilgisayarın tekil ağ cihaz numarasını (Mac adres) bilgilerinin loglarının tutulması, Kullanıcı web erişim olaylarının toplanması, oluşan logların bütünlük değerinin (hash) zaman damgası ile saklanması gerekmektedir.

3.3.11. Bu alıma konu olan Firewall, IPS ve Gateway antivirüs, web erişim mekanizmaları tarafından üretilen logları syslog protocol'ü üzerinden toplayabilmelidir.

3.3.12. Güvenlik duvarı üzerinde oluşan web erişim&firewall log kayıtlarında client cihazların kaynak mac adresi,kullanıcı adı(mevcutsa), kaynak ip adresi, hedef ip adresi, hedef port ve zaman bilgileri bulunmalıdır.

3.3.13. Güvenlik duvarı üzerinde oluşan web erişim log kayıtlarında http/s ve dns log kayıtları bulunmalıdır. HTTP için tutulan log kayıtlarında URL adresleri, HTTPS için tutulan log kayıtlarında paket içerisinden tespit edilen subdomain/domain adresleri, DNS için tutulan log kayıtlarında paket içerisinden tespit edilen subdomain/domain adresleri bulunmalıdır.

3.3.14. Güvenlik duvarı üzerine omurga switch'ten yönlendirilecek gelen trafiğin log kayıtları saklanırken client cihazların mac adresleri log kaydında bulunmalıdır.

3.3.15. Güvenlik duvarı üzerindeki client cihazlara ait DHCP ve ARP kayıtları belirli aralıklarla log kaydına alınmalıdır.

3.3.16. Üst maddelerde belirtilen log kayıtları 5651 sayılı kanuna uygun log tutulabilmelidir. Tutulan log kayıtları 5070 sayılı kanuna uygun olarak imzalanarak saklanmalıdır.

3.4. MİSAFİR AĞ KİMLİK DOĞRULAMA ARACI (HOTSPOT)

3.4.1. Türkkuşu Kampüsünde en az 150 (yüzelli) misafir kullanıcının aynı anda internet çıkışı yapabilmesi için yetkilendirilmelerini ve 5651 sayılı kanun gereği erişim kayıtlarının tutulabilmesini destekleyecek bir çözüm önerilecektir.

3.4.2. Hotspot üzerinde TC Kimlik / SMS / TC Kimlik ile beraber SMS/ LDAP-AD / Tek kullanımlık şifre/ Misafir Girişi vb. doğrulama metotları bulunmalıdır.

3.4.3. Sistem veya Yazılım üzerinde Mernis üzerinden TC Kimlik sorgulama ile kullanıcıyı doğrulayabilmelidir.

3.4.4. Teklif edilen ürün fiziksel ya da sanal platformda çalışabilmelidir. VmWare ya da Hyper-V sanallaştırma platformları desteklenmelidir. Fiziksel makine üzerine kullanılacaksa ayrı bir işletim sistemi veya lisansı gerektirmemelidir.

3.4.5. Sistem veya Yazılım üzerinde LDAP/AD üzerinden kullanıcı bilgilerini doğrulayarak kullanıcıya internet erişimi verebilmelidir.

3.4.6. Sistem veya Yazılım üzerinde SMS ile kullanıcılara doğrulama pin kodu göndererek kullanıcıyı doğrulayarak internet erişimi verebilmelidir.

3.4.7. SMS metni özelleştirilebilmelidir. SMS sağlayıcılarla API entegrasyonu bulunmalıdır.

3.4.8. Sistem veya Yazılım üzerinde izinli MAC sistemi oluşturulabilmelidir.

3.4.9. Sistem veya Yazılım Layer 2 modunda MAC Filtreleme özelliğine sahip olmalıdır.

3.4.10. Hotspot üzerinden oturum açan kullanıcıların tutulan log kayıtlarının (firewall, web, ips/ids gibi) tamamında kullanıcı adı eşleştirilerek 5651 sayılı kanuna uygun tutulmalıdır.

3.4.11. Hotspot oturum ekranına özelleştirilmiş logo eklenebilmelidir.

3.4.12. Hotspot oturum ekranında kullanıcıların onaylayabileceği KVKK onay metni olmalıdır.

3.4.13. Hotspot oturum ekranı birden fazla oturum açma seçeneğini aynı anda desteklemelidir. (Ör: TC Kimlik Doğrulama + LDAP/AD doğrulaması)

3.4.14. Hotspot girişi yapan kullanıcıların giriş ve çıkış saatleri listelenebilmelidir.

3.4.15. Kullanıcı giriş yaptıktan sonra istenilen web sitesine yönlendirme yapılabilmelidir.

3.4.16. Sistem veya Yazılım üzerinde bağlanan kullanıcıların MAC adresi bazlı veya kullanıcı doğrulama (kullanıcı / şifre denetimi) yoluyla internet erişimlerine izin verme veya engelleme imkânı tanımalıdır.

3.5. LİSANSLAMA VE GARANTİ SÜRESİ

3.5.1. Önerilen çözüm 3 (üç) yıl boyunca antivirüs, içerik ve uygulama filtreleme, saldırı tespit ve engelleme, VPN lisanslarının güncellemelerini alabilmelidir.

3.5.2. Bu şartname kapsamındaki cihazlar en az 2 (iki) yıl süre ile donanım garantili olacaktır.

3.5.3. Teklif edilecek cihazların kurulumları yapıldıktan sonra kurulan şartname kapsamında kurulan tüm sistemler için 3 (üç) yıl süre ile bakım destek hizmeti de sağlanacaktır. Yüklenici, teknik şartnameye uygun olarak iletilen problemlerin çözümüne ilişkin öncelikle uzaktan, gerekli görülen hallerde İdare ile koordineli olarak yerinde destek sağlayacaktır.

Funda YILMAZ Uzman	Yüksel SABUNCU Uzman	Cem Ali DÜNDAR Mühendis