TEKNİK ŞARTNAME

AĞ(NETWORK) SİSTEMLERİ VE GÜVENLİK DUVARI

KSÜ
SAĞLIK UYGULAMA VE ARAŞTIRMA HASTANESİ
AĞ(NETWORK) YEDEKLEME VE GÜVENLİK DUVARI
TEKNİK ŞARTNAMESİ

1.Genel Şartlar ve Garanti/Bakım Hizmetleri Kapsamı

1.1. Yüklenici Firma Tablo-1'deki temini yapılacak cihazlar için en az 2 yıl garanti ve garanti süresi boyunca 7/24/365 esasınca bakım ve destek hizmetlerini sağlayacaktır.

1.2. Yapılacak işin ve projeyle ilgili tüm süreçlerin Standartlara uygun şekilde yapılabilmesi amacıyla istekli firma aşağıdaki kalite ve standardizasyon belgelerine sahip olacaktır:

a.TS ISO/IC 27001:2017 Bilgi Güvenliği Yönetim Sistemi

b.Kamu Bilişim Yetki Belgesi

c.Kurumumuz Topoloji ve altyapısı Bilgi İşlem yetkililerimizle birlikte etüt edilerek, Güvenlik sisteminin kurulum ve konfigürasyonu yukarıda anılan güvenlik fonksiyonları aktif olarak kullanılacak şekilde yapılacaktır.

d.Yüklenici firma mevcut yapıda Üniversite tarafında çalışan santral, mail, web hizmetlerinin çalışmasına uygun firewall yapılandırması yapmalıdır.

e.Yüklenici firma Ağ yapılandırma kapsamında Dhcp, Voice Vlan, Dhcp trust ve Vlan Ayarlarını gözden geçirerek güvenli haliyle yeniden konfigüre etmelidir.

f.Yüklenici firma, teklif ettiği cihazın kurulumunu yapacak, eğitimini verecek personeli kendi bünyesinde çalışan elaman olmalıdır, kurulum ve eğitim üçüncü firma ya da firmalar tarafından yapılmamalıdır.

g.Yüklenici firma kurulum sırasında kurumumuz tarafından belirtilen 2 kişiye
2 gün süreyle en az Fortinet NSE 4 sertifikasına sahip personel tarafından cihaz kullanım eğitimi verecek, ayrıca 1 yıl 5 x 8 uzak bağlantı ve telefon desteği verecektir.

h.Sistemi kuracak olan istekli firma teklif ettiği ağ güvenliği ve sunucu sistemleri konusunda en az çözüm ortağı sertifikasına sahip olmalı, firma bünyesinde en az 2 adet üreticiden alınmış uzmanlık sertifikası olan personel bulunmalıdır. Kurulumu ve konfigürasyonları bu personeller yapmalıdır.

i.İstekli firma teklif ettiği ürünler için üretici veya distribütörden alınmış yetki belgelerini teklif dosyasında sunmalıdır.

1.3.Kurumda kullanılan Extreme Management Center yazılımı ile tam uyumlu cihazlar teklif edilmelidir.

1.4.Garanti ve Bakım Hizmetleri ile ilgili detaylar aşağıda belirtilmektedir:

a.Bakım ve destek hizmetleri kapsamındaki ağ cihazlarının arıza giderici bakım-onarım hizmetleri, ayrıca koruyucu bakım, onarım ve firmware yazılım güncellemeleri ile ağ yapılandırmasını geliştirmeye yönelik teknik destek hizmetleri sunulmalıdır.

b.Kurum Garanti ve Bakım kapsamına giren bütün cihazlar veya yazılımlar üzerinde bir proje kapsamında yeni bir özelliği aktif edeceği zaman firma personelinden yardım isteyebilir. Bu durumda firma personeli en geç 48 saat içerisinde ilgili özelliğin aktif edilebilmesi için gerekli adım adım teknik dokümanı sağlamalı ve eğer kurum personeli isterse bizzat çalışmaya katılmalıdır.

c.Ağ yapılandırmasında kullanılan cihazlarda sunulmakta olan bilgi güvenliği arttırıcı DoS/DDoS önleyici, ağ trafiğinin kilitlenmesini önleyici STP loop protect, DHCP snooping vb. özelliklerin saptanarak etkin hale getirilmesi için gereken her türlü teknik destek hizmetleri sunulmalıdır.

d.İdare'nin ağ ortamındaki veri trafiğinin paket çarpışma oranlarını optimum hale getirecek sanal ağ tanımlamalarının yapılması için gereken her türlü çalışmalar gerçekleştirilmelidir.

e.Ağ ortamında uçtan uca performans testleri gerçekleştirilerek elde edilen ağ durum raporlamaları İdareye her periyodik bakımda sunulmalıdır.

f.Ortak çalışmalar yürütülerek, kararlaştırılacak bir sıralama ve zaman planına göre, ağ yapılanmasının çeşitli bileşenlerinin iyileşmesine (optimizasyonuna) yönelik düzenlemeler yapılmalı ve belgelendirilmelidir.

1.5.Firma olarak arızaların takibi için kurumun mail atabileceği ve yasal anlaşmazlıklar sırasında geçerli olacak bir mail adresi bildirecektir.

1.6.Firma arıza sırasında arızayı çözmekle sorumlu personel/personellerinin telefon numarasını kuruma bildirecektir.

1.7.Arızanın başlangıç süresi; idarenin firmaya arızayı e-posta veya telefon ile bildirmesi ile başlayacaktır.

Tablo-1

SIRA	MALZEME	Birim	Miktar
1	Omurga Anahtar Kart	Adet	3

2.Omurga Anahtar Kart

2.1.Kurum bünyesinde kullanılmakta olan Extreme Networks S8 şasi ile uyumlu 3 adet kart teklif edilecektir.

2.2.Cihaz üzerinde teklif edilen tüm birimler orjinal olacak kesinlikle OEM ürünler teklif edilmeyecektir.

2.3.Teklif edilecek Fabric kart SK8008- 1224-F8 model Fabric kart teklif edilecektir. Fabric kartın Throughput değeri 960 Mpps olmalıdır.

2.4.Teklif edilecek I/O modüller SK8008-1224 modelinde olmalı ve Fabric kart ile uyumlu olmalıdır.

2.5.Teklif edilecek kartlar üzerinde en az 48 Port 10 Gigabit-Base-X SFP+ port bulunacaktır. 48 port 10 Gigabit yedeklilik amacıyla cihazda en az 2 farklı kart ile birlikte teklif edilecektir. Ayrıca cihaz ile birlikte en az 1 adet Fabric Modül önerilecektir. Teklif edilecek tüm portlar wire-speed/non-blocking (tıkanmasız) olarak önerilecektir. Teklif edilecek kartlar ile birlikte 4 adet 10G LR SFP+ ve 3 adet 1G Bakır SFP teklif edilecektir.

3.AĞ ve GÜVENLİK DUVARI SİSTEMİ

Ağ Güvenlik Duvarı aşağıda belirtilen güvenlik fonksiyonlarını ve teknolojilerini sağlamalıdır.

3.1.Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari;

3.1.1.Güvenlik Duvarı (Firewall)
3.1.2.IPSec VPN Sonlandırma Sistemi
3.1.3.SSL VPN Sonlandırma Sistemi
3.1.4.Saldırı Tespit ve Engelleme Sistemi (IPS)
3.1.5.Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
3.1.6.Virüs/Zararlı İçerik Kontrolü
3.1.7.URL Kategori Filtreleme
3.1.8.Bant genişliği yönetimi

Özelliklerine sahip olmalıdır.

Erdoğan YILDIRIM
KSÜ SAĞ. Hastanesi
Bilgi İşlem

3.2.Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlamalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.

3.3.Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, her hâlükârda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.

3.4.Teklif edilen Ağ Güvenlik Duvarı High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmeli ve cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.

Halil İbrahim ÇALIŞIR
Bilgi İşlem Sorumlusu

Abdulkadir KOZANOĞLU
KSÜ SUAH.
Bilgi İşlem Birimi

3.5.Yedeklilik konfigürasyonunda her segment için güvenlik duvarı üzerinde set edilecek IP sayısı 1 (bir) adet olmalıdır. Bu sayede modüller için ayrı, cluster IP si için ayrı IP adreslerinin kullanımına gerek kalmamalıdır.

3.6.Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.

3.7.Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır

3.8.Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN'lar arayüz (interface) olarak kullanılabilmelidir.

3.9.Sistem Sanal Güvenlik Duvarı özelliği ile kullanıldığı durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilmelidir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilmelidir.

3.10.Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.

3.11.Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır;
- 3.11.1.SPI (stateful packet inspection),
- 3.11.2.Saldırı Tespit ve Engelleme Sistemi (IPS)
- 3.11.3.Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
- 3.11.4.Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü
- 3.11.5.URL Kategori Filtreleme

3.12.Routing modda aşağıdaki özellikleri sağlamalıdır;
- 3.12.1.SPI (stateful packet inspection),
- 3.12.2.IPSec VPN Sonlandırma,
- 3.12.3.SSL VPN Sonlandırma,
- 3.12.4.Saldırı Tespit ve Engelleme Sistemi (IPS)
- 3.12.5.Uygulama Tanıma ve Kontrolü (Application Control) Sistemi
- 3.12.6.Virüs/Zararlı İçerik Kontrolü
- 3.12.7.URL Kategori Filtreleme
- 3.12.8.Bant genişliği kontrolü
- 3.12.9.Statik yönlendirme (static routing),
- 3.12.10.RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.
- 3.12.11.Sunucu yük dengeleme
- 3.12.12.WIFI Access Point kontrolcüsü
- 3.12.13.WAN optimizasyon
- 3.12.14.Web Cache

3.13.Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli ve/veya aynı anda kullanabilmelidir.

3.14.Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.

3.15.Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.

3.16.Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü ve/veya zone bazlı yazılabilmelidir.

3.17.Güvenlik duvarı politikaları, kullanıcı grupları bazında yazılabilmeldir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.

3.18.Kullanıcı bazında NAT kuralı yazılabilmelidir.

3.19.Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.

- 3.19.1.Kaynak, hedef ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.
- 3.19.2.Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.
- 3.19.3.İstenildiğinde tek IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural dahilinde izin verilmiş olan tüm kaynak IP lerin herbiri için, tanımlanan bant genişliğinin ve/veya max eşzamanlı oturum sayısının garanti edilmesi sağlanmalıdır.
- 3.19.4.Aynı kural dahilinde izin verilen her kaynak için, tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.
- 3.19.5.Uygulama bazında bant genişliği kontrolü yapabilmelidir.
- 3.19.6.Aynı trafik ile ilgili Inbound ve outbound doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.

3.20.Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.

3.21.Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları gibi tanımlı en az 3.000 (üçbin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.

3.22.Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir

3.23.Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır.

3.24.IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilmelidir.

3.25.Teklif edilen sistem istenilen atak türleri gerçekleştiğinde bu atakları sadece engellemekle kalmayıp, atak kaynağını belli bir süre engelleyebilecek şekilde yapılandırılabilmelidir. Bu sayede atak yapan IP adresinin olası diğer saldırıları başlamadan engellenmiş olmalıdır.

3.26.Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkân sağlamalıdır.

3.27.Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir

3.28.Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.

3.29.Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.

Erdoğan YILDIRIM
KSÜ ... Hastanesi
Bilgi İşlem

Halil İbrahim ÇALIŞIR
Bilgi İşlem Sorumlusu

Abdulkadir KOZANOĞLU
KSÜ SUAH
Bilgi İşlem Birimi

3.30.SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.

3.31.SSL VPN özelliği en az 5.000 kullanıcı lisansı ile teklif edilecektir.

3.32.SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.

3.33.SSL VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, Bant Genişliği yönetimi (QoS) özellikleri uygulanabilir olmalıdır.

3.34.Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3 trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilmelidir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir

3.35.Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.

3.36.Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.

3.37.Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı URL filtreleme politikaları set edilebilmelidir

3.38.Sistem üzerinde en az 60 adet URL kategorisi bulunmalıdır.

3.39.Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.

3.40.Çözüm sıfır-gün ataklarına karşı, bulut tehdit engelleme sistemleri ile entegre olmalı, bu sayede koruma seviyesini arttırmalı ve potansiyel hatalı tespit sayılarını azaltabilmelidir. Sıfır-gün ataklarına karşı koruma sağlamak için, Firewall'lar üzerine eklenebilecek bulut tehdit engelleme sistemleri lisansları 3 YIL geçerli olacak şekilde teklif edilmelidir.

3.41.URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilmelidir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.

3.42.İstenildiğinde kategorilerden bağımsız olarak, sisteme eklenebilecek tam URL bilgisi (Örneğin: www.abc.com/deneme/sayfa1.php) bazında engelleme yapabilmelidir.

3.43.Https üzerinden erişilmeye çalışılan domain adreslerinin (örneğin www.abc.com) engellemesi sertifika kullanımı olmadan gerçekleştirilebilmelidir.

3.44.SSL trafiğini kendi üzerinde yaratılan bir sertifikayı yada farklı bir CA den alınmış yeterli özelliklere sahip bir sertifika ile inceleyebilmelidir. Bu sayede sadece domain bazında değil, URL bazında (Örneğin: www.abc.com/deneme/test.php) engelleme yapabilmelidir. URL kategorileri bazında SSL incelemeye girmeyecek domainler belirlenebilmelidir.

3.45.URL filtreleme uyarı ekranları özelleştirilebilecektir.

3.46.Teklif edilen tüm 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 ve Ping6 desteklenmelidir.

3.47.Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilmelidir:
- 3.47.1.Seri bağlantı ile konsol port üzerinden,
- 3.47.2.Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden
- 3.47.3.SSH bağlantı ile komut satırı (commandline) üzerinden

3.48.Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir

3.49.Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.

3.50.Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.

3.51.Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, güncel "Network Firewalls" için "Gartner Magic Quadrant" tablosunda yer almalıdır.

3.52.Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.

3.53.Teklif edilen güvenlik sistemi, aynı zamanda yük dengeleyici özelliklerine sahip olacaktır.

3.53.1.Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP, Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.
3.53.2.Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.
3.53.3.HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi sağlanabilmelidir.
3.53.4.SSL bağlantıları için SSL Offloading özelliği olmalıdır.
3.53.5.Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:
- 3.53.5.1.Kaynak Ip hash bilgisi
- 3.53.5.2.Round robin
- 3.53.5.3.Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak
- 3.53.5.4.Aktif durumda olan gerçek sunucudan ilkine trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderimesi
- 3.53.5.5.Ping paketlerine verilen cevaplar esas alınması
- 3.53.5.6.Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak

3.53.6.Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin http://10.31.101.30/test_page.htm adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.

3.54.Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.

3.55.Teklif edilen sistem wifi controller olarak çalışabilecek, bu sayede kullanılabilecek kablosuz erişim cihazlarının yönetimi için kullanılabilecektir.

3.56.Wan optimizasyon özelliklerine sahip olacaktır.

3.57.Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.

Erdoğan YILDIRIM
KSÜ SUAH Hastanesi
Bilgi İşlem

Güvenlik Duvarı Performans Değerleri

3.58.Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda en az 70 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.

3.59.Her bir Ağ Güvenlik Duvarı ünitesi Tehdit Koruma (Firewall + IPS + Uygulama Denetimi + Antimalware) özellikleri aktifken en az 9 Gbps kapasiteli olmalıdır.

Halil İbrahim ÇALIŞIR
Bilgisayar Mühendisi

Abdulkadir KOZANOĞLU
KSÜ SUAH
Bilgi İşlem Birimi

kullanıcı/istemci arasındaki istek-cevap trafiğinin toplamına (çift yönlü analiz ile) bu güvenlik özelliklerinin uygulandığı konfigürasyonda belirlenmiş olmalıdır. Belirtilen bu değer ürün kataloglarında yer almalıdır. Ürün kataloglarında Tehdit Koruma için farklı terminoloji kullanılmış ise bu koşulda ürün kataloğunda NGFW (Firewall + IPS + Uygulama Denetimi) kapasitesi gerçek ortam değeri baz alınarak en az 10 Gbps olmalıdır.

3.60.Sistem aynı anda en az 7,5 milyon oturumu desteklemeli ve saniyede en az 500.000 yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili dokümanlarında belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.

3.61.Güvenlik Duvarı Sistemi en az 50 Gbps IPSec VPN throughput 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.

3.62.Sistem Site-to-Site için en az 2.000 adet, Client to site için 50.000 adet IPSec VPN tünel desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir.

3.63.Sistem 12 Gbps IPS throughput performans 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.

3.64.Sistem üzerinde;
3.64.1.En az 8 adet 10GE SFP+ ara yüz bulunmalıdır.
3.64.2.En az 8 adet 1GE SFP ara yüz bulunmalıdır.
3.64.3.En az 16 adet 1GE RJ45 ara yüz bulunmalıdır.

3.65.Sistem Syslog Sunuculara ve Kayıt/Raporlama Sistemine kayıt gönderebilmelidir.

3.66.Sistemin; Firewall ve 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.

4.KAYIT VE RAPORLAMA SİSTEMİ

4.1.Önerilen güvenlik duvarı sisteminin kayıt depolama ve takibini, raporlama işlemlerini gerçekleştirmek için aşağıda belirtilen şartlara uyan kayıt takip ve raporlama ürün/ürünleri alınacaktır.

4.1.1.Aşağıda belirtilen özellikler yönetim ve kayıt sistemlerinin ayrı veya tek bir sistem olarak önerilmesi durumunda da sağlanacaktır.

4.1.2.Önerilen sistem, saniyede en az 5 GB/Gün log kayıt alabilmelidir.

4.1.3.Log kayıt alanı olarak en az 3 TB depolama alanını desteklemelidir.

4.1.4.Herhangi bir anda kurulmuş olan bağlantıları gerçek zamanlı olarak izleyebilme olanağı olacaktır.

4.1.5.Cihaz üzerinden geçen tüm trafiğin günlüklerde tutulması, istenen kıstaslara göre (En az IP, IP aralığı, ağ, protokol, zaman) filtrelenebilmesi ve aktif bağlantıların gerçek zamanlı izlenebilmesi sağlanacaktır.

4.1.6.Gün, saat veya haftalık periyodlarda yapılandırılabilen otomatik kayıt arşivleme özelliği olacaktır.

4.1.7.Güvenlik duvarları ile kayıt sunucusu arasında iletişimin sağlanamaması durumunda oluşturulan kayıtlar, bağlantı sağlanana kadar güvenlik duvarının kendi üzerinde tutulabilmelidir.

4.1.8.Yönetilen ağ güvenlik duvarlarına ait performans ve güvenlik duvarları üzerinden geçen trafik ile ilgili bilgileri geçmişe yönelik olarak gösterebilme özelliği desteklenecektir.

4.1.9.Merkezi yönetim dâhilinde bulunan bileşenlere ait anlık ortalama CPU, boş disk alanı, firewall, firewall cluster üzerinden akan tüm uygulamalar, kullanıcı IP adresleri ve dâhili kullanıcı isimleri gibi değerler anlık ve sürekli olarak görüntülenebilecektir.

4.1.10.Önerilen kayıt yönetim sistemi geçmişe yönelik olarak raporlama yapabilme özelliğine sahip olacaktır. Örneğin bant genişliği kullanımı, uygulama denetimi, URL filtreleme ile ilgili istenen tarih aralıklarında raporlar üretebilecektir.

4.1.11.Tutulan kayıt alanları baz alınarak özelleştirilmiş sorgular yazılabilmeli ve bu sorguların çıktıları, tablo, pie-chart şeklinde raporlar içerisine konulabilmelidir.

4.1.12.Pdf formatında rapor üretebilmeli ve üretilen raporları belirtilen e-mail adreslerine otomatik veya elle gönderebilmeli, ftp veya web sitelerine otomatik olarak yükleyebilmelidir.

4.1.13.Kayıtları ftp veya benzer bir protokolle harici bir Sunucu veya Depolama alanı üzerinde yedekleme yapıp arşivleyerek kayıtların yedekliliği sağlayabilmelidir.

4.2.Yukarıda belirtilen seçeneklerden hangisi ile teklif edilirse edilsin, teklif edilen sistemlerin en az 3 yıl yazılım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.

5.KİMLİK DOĞRULAMA SİSTEMİ VE KAPASİTE

5.1.Teklif edilen ürün 1.000 adet anlık local veya uzak kullanıcı desteğine sahip olmalıdır.
5.2.Teklif edilen ürün 50 adet CA (Certificate autority) desteğine sahip olmalıdır.
5.3.Teklif edilen ürün 1.000 adet kullanıcı sertifika desteğine sahip olmalıdır.
5.4.Teklif edilen ürün 1.000 adet kullanıcı grubu oluşturma desteğine sahip olmalıdır.
5.5.Teklif edilecek ürün donanım olarak veya sanal olarak VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0 / 5.5 / 6.0, Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2 ortamlarında çalışabilmelidir.
5.6.Teklif edilen ürün tek olarak lisanslanmalı ve gerektiğinde yedekli Active-Passive HA ve Config SyncHA desteğine sahip olmalıdır.

Kimlik Doğrulama Özellikleri
5.7. Teklif edilecek ürün SSO (single sign on) desteği olmalıdır ve aşağıdaki kaynaklardan beslenebilmelidir.
5.7.1 AD (Active directory) sorgulama (AD polling) veya AD agent iletişimi
5.7.2 TS (Terminal server) agent
5.7.3 Kerberos
5.7.4 REST API
5.7.5 Radius Accounting
5.7.6 FortiClient SSO client
5.7.7 SSO Login Portal
5.7.8 Syslog
5.8. Teklif edilecek ürün Windows altyapılar için WMI sorgulama yöntemi ile aktif olmayan kullanıcıları SSO listesinden çıkartabilmelidir veya belli bir süre limiti ile SSO listesinden çıkartabilmelidir.
5.9. Teklif edilecek ürün kablosuz altyapılar için merkezi kimlik doğrulama sistemine sahip olmalıdır.
5.10. Teklif edilecek ürün kablosuz altyapılar için kullanıcılar için PEAP, EAP-TTLS desteği olmalıdır aynı zamanda sertifika tabanlı EAP-TLS BYOD (bring your own device) desteğine sahip

Erdoğan YILDIRIM
KSÜ SUAH
Bilgi İşlem

Abdulkadir KOZANOĞLU
KSÜ SUAH
Bilgi İşlem Birimi

Halil İbrahim ÇALIŞIR
Bilgi İşlem Sorumlusu

olmalıdır.
5.11. Teklif edilecek ürün kablosuz altyapılar için mobil telefon doğrulamalı konuk yönetimi captive portal çözümüne sahip olmalıdır.
5.12. Teklif edilecek ürün kablosuz altyapılar için konuk captive portal çözümü admin onayı ile kullanıcı şifrelerini HTTP/HTTPS/mail-to-sms servislerine entegrasyonuna sahip olmalıdır.
5.13. Teklif edilecek ürün kablosuz altyapılar için konuk captive portal çözümü değiştirilebilir önyüz desteğine sahip olmalıdır.
5.14. Teklif edilecek ürün kablosuz altyapılar için SSO desteği ile Fortinet firewall'lara direk entegre olabilmelidir.
5.15. Teklif edilecek ürün kablosuz altyapılar için konuk yönetimi captive portal çözümü facebook, twitter, Google vb. Kimlik bilgileri ile giriş desteğine sahip olmalıdır.
5.16. Teklif edilecek ürün kablosuz altyapılar için konuk yönetimi belli bir sürede ilgili kullanıcıların resetlenmesini ve sistemden silinmesini desteklemelidir.
5.17. Teklif edilen ürün sertifika yönetimi yapabilmelidir.
5.18. Teklif edilecek ürün kullanıcı sertifika yönetimi aşağıdaki bağlantılar için oluşturup doğrulayabilmelidir.
5.18.1 VPN
5.18.2 Kablosuz 802.1X(PEAP,EAP)
5.18.3 Windows desktop authentication
5.18.4 FTK300 USB PKI Certificate Store uyumluluğu
5.18.5 Kablo NAC desteği 802.1X (PEAP, EAP-TTLS, EAP-TLS, EAP-GTC)
5.19. Teklif edilen ürün Radius Accounting Proxy desteği olmalıdır.
5.20. Teklif edilen üründe MAC cihaz kimlik doğrulama desteği olmalıdır.
5.21. Teklif edilen ürün harici AD, LDAP, Radius desteği olmalıdır.
5.22. Teklif edilen ürün LDAP server olarak kullanılabilmelidir.
5.23. Teklif edilen ürün Radius ürün olarak kullanılabilmelidir.
5.24. Teklif edilen ürün Token yönetimi yapabilmelidir. Lisans kadar soft veya hardware token register edilebilmelidir.
5.25. Teklif edilen ürün üzerinden adil kullanım kotası amaçlı kota temelli bant genişliği yönetimi yapılabilmelidir.

YÖNETİM ÖZELLİKLERİ

5.26. Teklif edilen ürün HTTPS üzerinden yönetilebilmelidir.
5.27. Teklif edilen ürün kullanıcı girişlerini kayıt altına alabilmeli ve harici loglama sistemlerine aktarabilmelidir.
5.28. Teklif edilen ürün CPU ve memory kullanımlarını, kullanıcı adet istatistiklerini önyüz üzerinden gösterebilmelidir.
5.29. Teklif edilen ürün otomatik backup alarak belirlenen zamanda harici ftp sitesine gönderebilmelidir.
5.30. Teklif edilen ürün SNMP v1/v2c ve v3 destegi olmalıdır. MIB bilgileri üzerinden soğulama yapılabilmelidir.
5.31. Teklif edilen ürün admin kullanıcılarına yetkilendirme yapılabilmelidir.
5.32. Teklif edilen ürün log kayıtları HTTPS arayüz üzerinden filtrelenebilir şekilde sorgulanabilmelidir.
5.33. Teklif edilen ürün log kayıtlarını harici syslog server'lara gönderebilmelidir.
5.34. Teklif edilen ürün 3 (üç) yıllık yazılım destek paketi ile verilmelidir.

Erdoğan YILDIRIM
KSÜ SUA Hastanesi
Bilgi İşlem

Halil İbrahim ÇALIŞIR
Bilgi İşlem Çalışanı

Abdulkadir KOZANOĞLU
KSÜ SUAH
Bilgi İşlem Birimi