2021-02 NETWORK SİSTEMİ ALIMI İHALESİ

TEKNİK ŞARTNAMESİ

1. ANA OMURGA ANAHTAR (2 Adet)

1) Anahtar, 19 (on dokuz) inç rack tipi kabinete monte edilebilecektir.
2) Tüm sistem ve bağlı donanımlar, 220 (iki yüz yirmi) V. ve 50 (elli) Hz. şebeke gerilimi ile beslenecek ve güç kabloları Türkiye şartlarına uygun olacaktır.
3) Anahtarlama cihazı, 0 (sıfır) °C ile +40 (artı kırk) °C arasındaki sıcaklıklarda ve bağıl nemi %10 (yüzde on) ile %85 (yüzde seksen beş) arasında olan ortamlarda sorunsuz çalışacaktır.
4) Anahtarın üzerinde en az 48 adet kesintisiz (line rate) 1/10 Gbps portları bulunmalı bu portlara, 1000BASE-LX/LH , 1000BASE-SX, 1000BASE-T, 10GBASE-SR, 10GBASE-ER SFP modülleri ve 10G Ethernet Bakır (Twinax) kablo yeterli metrajda kullanılmalı ve sonlandırılması yapılmalıdır. 2 ana omurga anahtar birbirlerine VPC ile bağlanacaktır.
5) Teklif edilen anahtar ağda bulunan diğer kenar anahtarlar ile aynı model (Cisco) ve eş değer kalitede olmalıdır.
6) Omurga anahtarların birbirleri ile yedekli bağlantısı için en az 1 metre uzunluğunda 2 adet DAC kablo teklif edilecektir.
7) Omurga anahtarların kenar anahtarlar ile bağlantısı için en az 3 metre uzunluğunda 4 adet DAC kablo teklif edilecektir.
8) Teklif edilecek omurga anahtar en az 3 yıl üretici destek paketi ile teklif edilmelidir.
9) Teklif edilecek omurga anahtar yedekli olarak yapılandıralacak ve 2 adet teklif edilecektir.
10) Anahtarın paket iletimindeki gecikme (Latency) en fazla 250 (iki yüz elli) nano saniye olacaktır.
11) Anahtarın switching (anahtarlama) kapasitesi en az 960 (dokuz yüz altmış) Gbps olmalıdır.
12) Anahtarın bekletmeden iletim (cut-through) yeteneği olacaktır.
13) Anahtarın üzerinde istenildiğinde yazılım arttırımı ile NAT / PAT protokolleri, Statik NAT, dinamik NAT, PTP (precision time protokolü) bulunmalıdır, NAT'ı donanım olarak (hardware üzerinde) desteklemelidir.
14) Anahtarda, port başına düşen tampon bellek (buffer) 5 MByte a kadar dinamik olarak artırılabilmelidir.
15) Anahtar, multicast ve unicast trafik için farklı kuyruklama mekanizmalarına sahip olmalıdır, QOS (Quality of Services) için en az 8 (sekiz) adet kuyruk bulunmalıdır.
16) Anahtar RFC 3168'i desteklemelidir.
17) Anahtar RIPv2,VRRP, en az 256 route'a kadar OSPFv2, Multicast sparse mode (PIM-SM), PIM source-specific multicast (PIM SSM), Bidirectional PIM (PIM-Bidir) ve Multicast Source Discovery Protocol (MSDP) desteklemelıdır.
18) Anahtar istenmesi durumunda lisans arttırımı ile BGP, OSPFv2, PBR (politika tabanlı yönlendirme) desteklemelidir.
19) Anahtarın; yönlendirici erişim listesi (RACL), VLAN erişim listesi (VACL), port temelli erişim listesi (PACL) ve Dynamic Host Configuration Protocol (DHCP) Snooping desteği bulunmalıdır.

20) Anahtar üzerindeki mikroişlemci (CPU) en az iki çekirdekli ve en az 1.5 Ghz hızında, en az 4 (dört) GB bellek kapasitesinde olmalıdır.
21) Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için port mirroring desteği bulunmalıdır. Birden fazla kaynak portu, hedef portuna aynalanabilmelidir.
22) Anahtarda control plane'i koruyucu CoPP (control plane policing) gibi mekanizmalar bulunmalıdır.
23) Anahtar IEEE 802.1p protokolünü destekleyecektir.
24) Anahtar, jumbo frame desteğine sahip olacak, desteklenen jumbo framelerin uzunluğu en az 9216 (dokuz bin iki yüz on altı) byte olacaktır.
25) Anahtar, en az bir adet RS-232 konsol portuna ve en az bir adet 10/100/1000BASE-T management portlarına sahip olacaktır.
26) Anahtarın üzerinde güç kaynakları ve fan yedeklenebilir olmalıdır.
27) Anahtar IPv4 route tablosu kapasitesi en az 24000, l3 multicast tablosu kapasitesi en az 8000, MAC adres tablosu kapasitesi en az 64000 olmalıdır.
28) Anahtarın, Rapid Spanning Tree Protokolü(RPVST+) veya VSTP, Multi Sppanning Tree Protokolü(MST), Link Layer Discovery Protokolü (LLDP), Storm Control, Link Aggregation Control Protokol (LACP, IEEE 802.3ad, IEEE 802.1ax) desteği olacaktır.
29) Anahtarın NTP (Network time Protokol) server özelliği bulunmalıdır, böylelikle anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecektir.
30) Anahtarda Q-in-Q desteği bulunmalıdır.
31) Anahtarda, ihtiyaç olduğunda lisans arttırımı ile vrf-lite'ı desteklemelidir.
32) Anahtarlama cihazı, kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır. Bu amaçla kullanılan protokol, ağ üzerindeki diğer tüm anahtarlarda da desteklenecektir.
33) Anahtarda 802.3x flow control desteği bulunmalıdır.
34) Anahtarın IGMP Snooping özelliği olacak ve tablosu en az 8000 (sekizbin) kapasiteli olacaktır.
35) Anahtarda en az 4000 adet Vlan tanımlanabilecektir. Yeni VLAN yapısı oluşturulacak ve Firewalla taşınacaktır.
36) Anahtarda 32 Eşit Yüklü Çoklu Yönlü (ECMP) tanımlanabilecektir.
37) Anahtarın anahtarlama performans değeri en az 720 Mpps olmalıdır.
38) Anahtar, bir scripting arayüzüne sahip olacak, kullanıcı tarafından önceden tanımlanmış değerler ve komutlar ile proaktif eylemler tanımlanabilecektir.
39) Anahtar istenmesi durumunda lisans arttırımı ile grafik tabanlı bir ağ yönetim platformu tarafından yönetilebilmelidir.
    a. Anahtarın firmware güncellemesi FTP ya da TFTP yardımı ile yapılabilecektir.
40) UDLD (unidirectional link dedtection) tek taraflı link tespiti özelliği ile loop engelleyici mekanizmaya sahip olmalıdır.
41) Anahtarda oturum açmak için Radius ve TACACS+ protokolü ile yetkilendirme yapılabilmelidir.
42) Anahtar, SNMP v1, v2, v3, telnet, Secure Shell (SSH) v2, ve konsol aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
43) Detaylı gerçek zamanlı trafik analizi yapabilmek için port mirroring desteği bulunmalıdır. Birden fazla kaynak portu, hedef portuna aynalanabilmelidir. Aynı anda en az 8 adet port mirroring oturumu desteklenecektir.

44) Aynı LAN'daki farklı bir anahtar üzerindeki port da kaynak portu olarak seçilebilmelidir. (remote port mirroring).
45) RMON ve Syslog desteği bulunmalıdır.
46) Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden geçirebilmelidir (standart ve extended IP access control lists). Bu listeler zamana bağlı olarak aktif ya da pasif hale geçebilmelidir
47) Anahtarın konsol port erişiminde farklı seviyelerde yetkiler tanımlanabilecektir. Bu sayede yetkilendirme sonrası, cihaza farklı seviyelerde (kısmi yönetim, tam yönetim, izleme gibi) erişim sağlanabilecektir.
48) Anahtarın, IGMP snooping, IGMP filtreleme özelliği bulunacaktır, bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
49) Anahtarın BPDU (Bridge Protocol Data Unit) Guard özelliği bulunacaktır. Bu sayede Spanning Tree grubunda olmayan portlara, o grubun BPDU paketlerinin girişi engellenecektir.
50) Anahtarın Spanning Tree Root Guard (STRG) özelliği bulunacaktır. Bu sayede network yöneticisinin kontrolünde olmayan anahtarların, Spanning Tree protokolü için root anahtar olması engellenebilecektir.

2. BAKIR OMURGA ANAHTAR (4 Adet)

1) Anahtar üzerinde 48 adet 10/100/1000 BaseT gigabit ethernet portu ve en az 4 adet SFP+ bulunmalıdır. Bu yuvalar, 100BaseFX, 1000BaseSX, 1000BaseLX, 1000BaseLH, 10G SR, 10G LR GBIC modülleri ile doldurulabilmelidir.
2) Teklif edilecek kenar anahtar en az 3 yıl üretici destek paketi ile teklif edilmelidir.
3) Teklif edilecek anahtar kenar ve omurga anahtarlar ile aynı marka olması tercih sebebidir.
4) IEEE 802.3, 802.3u, 802.3ab, 802.3z standartları desteklenmelidir.
5) Anahtarlama kapasitesi en az 175 Gbps olmalıdır. Anahtarın L2 anahtarlama performans değeri en az 130 Mpps olmalıdır.
6) Anahtarlar yığınlanabilir yapıda olmalıdır. En az 4 adet anahtar yığınlanabilir yapıya dahil edilebilmeli ve en 4 adet 10G DAC kablo ile teklife dahil edilmelidir.
7) Yığınlanabilir bağlantılar için en az 4 adet 2 metre 10G DAC kablo teklife dahil edilecektir.
8) Anahtar üzerinde 256 MB flash ve 512 MB CPU memory bulunmalıdır.
9) Anahtar üzerindeki MAC adres tablosunda en az 16000 adet MAC adresi tutabilmelidir.
10) Anahtarın Time Domain Reflectometry (TDR) desteği olmalı böylece bakır kablonun karakteristiğini ve kalitesini test edebilmelidir.
11) Anahtar, port security ve 802.1x özelliklerini desteklemelidir.
12) Anahtar, IEEE 802.1x protokolünü kullanarak, radius server yardımı ile port bazında kullanıcı yetkilendirmeyi desteklemelidir
13) Anahtarın, DoS saldırılarına karşı koruma sağlayan "DoS Prevention" ve "SYN-FIN protection" desteği bulunmalıdır.
14) Anahtarın 802.1Q desteği olmalıdır. Desteklediği VLAN sayısı en az 4000 olmalıdır.

15) Anahtarın, ses trafiğini, özel bir vlan kullanarak uygun QoS seviyesi belirlemesini sağlayan voice vlan desteği bulunmalıdır. Ayrıca voice vlan'ın, komşu cihazların CDP veya LLDP iletilerinden elde ettiği voice vlan bilgisi ile belirlenmesini sağlayan "Auto Voice VLAN" desteği bulunmalıdır.
16) Anahtarın Generic VLAN Registration Protocol (GVRP) ve Generic Attribute Registration Protocol (GARP) desteği olmalıdır.
17) Anahtar, IEEE 802.1d (STP) ve IEEE 802.1w (RSTP) ve 802.1s (MSTP) "spanning tree" protokollerini destekleyecektir.
18) Anahtarın IGMP V1,V2, V3 desteği olmalıdır ve en az 255 multicast group desteklemelidir.
19) Anahtar, CDP, LLDP ve LLDP-MED protokollerini desteklemelidir.
20) Anahtar, üzerinde 8 adede kadar 10/100/1000 portun bir grup altında toplanarak tek port gibi çalıştırılabilmesini sağlayan 802.3ad LACP (Link Aggregation Protocol) protokolünü desteklemelidir.
21) Anahtarın, cihaza giren frame sayısını sınırlandırarak broadcast, multicast ve bilinmeyen unicast adreslerden gelen frame' lerin yaratabileceği yoğun trafiği engelleyebilen "storm control" desteği bulunmalıdır.
22) Anahtarda, her bir port ve vlan için hız sınırlandırılmasını sağlayan "rate limiting" desteği bulunmalıdır.
23) Anahtarın DHCP Server özelliği bulunmalı.
24) Anahtar, DHCP option 12, 66, 67, 129 ve 150 desteklemelidir.
25) Anahtar, L3 statik routing desteklemelidir. En az 900 adet statik route yazılabilmelidir.
26) Anahtar üzerinde 128 IP interface oluşturulabilmelidir.
27) Anahtar, Classless Inter-Domain Routing desteklemelidir.
28) Anahtar, SNMP v1, v2c, v3, HTTP (web), konsol port , Telnet ve SSH aracılığı ile yönetilebilmeli ve gözlenebilmelidir.
29) Konsol Yönetim Platform - Anahtarların yönetimi için x86 mimariye sahip, üzerinde en az 8 konsol port ara yüzü, en az 4 port GBE ara yüzü bulunan, 4Gb RAM ve 32GB SSD sahip ayrıca 4 adet LTE sim kart desteği bulunan donanım temin edilmelidir.
30) Anahtar, Bonjour protokolünü desteklemelidir.
31) Anahtarın tüm portları en az 4 adet RMON grubunu (history, statistics, alarms, events) desteklemelidir.
32) Anahtarda, detaylı gerçek zamanlı trafik analizi yapabilmek için port ve vlan mirroring desteği bulunmalıdır. En az 4 adet kaynak portu ya da 4 adet vlan 1 hedef portuna aynalanabilmelidir.
33) Anahtar üzerinde en az 1024 adet Access Control Lists (ACLs) yazılabilmeli. Ayrıca zaman bazlı ACL desteği olmalıdır.
34) Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecektir. SNTP desteği olmalıdır.
35) Anahtarın, port ve vlan bazlı önceliklendirme – CoS desteği bulunmalıdır.
36) Anahtarın, IPv6 desteği bulunmalıdır.
37) Anahtarda IPv6 erişim listesi oluşturulabilmeli, böylece IPv6 trafiği bloklanabilmeli ya da sınırlandırılabilmelidir.
38) Anahtar, yönetim erişimi kimlik kontrolü için RADIUS desteklemelidir.

3. AĞ ERİŞİM KONTROL SİSTEMİ

1) Teklif edilecek sistem, en az politika yöneticisi, uygulayıcı sistemler bileşenlerinden oluşmalıdır ve kimlik denetimi, yetkilendirme, uyumluluk kontrolü, misafir erişimi, yönetimi, izlenmesi ve cihazların otomatik olarak trafik tiplerine göre profillendirmesi, sonrasında ise tanımlı rollere atanması işlemlerini birbiri ile tamamen uyumlu bir şekilde sağlayabilecektir. NAC çözümü bu amaç için üretilmiş olmalıdır.
2) Teklif edilecek sistem, yönetim, raporlama, politika ve kural tanımlama fonksiyonlarını sağlayacaktır.
3) Teklif edilecek sistem üzerinde tüm yetkilendirme ve izin verme süreci detaylı olarak loglanacak ve bu loglar üzerinde tüm süreç takip edilebilecektir.
4) Teklif edilecek sistem kurumsal ağ altyapısına erişmek için girişimde bulunan son kullanıcı cihazlarına (bilgisayar, tablet, cep telefonu, yazıcı gibi), dinamik olarak erişim izni verebilecek ya da engelleyebilecektir.
5) Teklif edilecek sistem agent ile ve agent olmadan çalışmayı destekleyecektir.
6) Teklif edilecek sistem kendi üzerinde sertifika yaratıp kullanabilecektir. Ayrıca harici bir Certificate Authority (CA) in oluşturduğu sertifikaları da kullanabilecektir.
7) İstenmesi halinde ileride sisteme yeni yazılım veya lisans ilavesi ile son kullanıcı cihazları için profiller ya da roller, her profil ya da rol için farklı kurallar ve her kural için de farklı kontroller tanımlanabilecektir.
8) Misafir kullanıcılar için Agentless (ajansız) Web tabanlı kimlik doğrulama ve sonrasında yetkilendirme desteklenecektir.
9) Aynı anda birden fazla kimlik doğrulama sunucusunu desteklenecektir.
10) Yönetim sunucusunun detaylı raporlama özellikleri bulunacak ve istenmesi durumunda bu raporlar API'ler ile harici bir sunucuya ya da kayıt ortamına alınıp saklanabilecektir.
11) Yönetim sunucusu üzerinden merkezi olarak alınacak raporlar aşağıda belirtilen bilgileri içerecektir.
    i. Kimlik doğrulamadan geçen kullanıcılar
    ii. Kimlik doğrulamadan geçemeyen kullanıcılar
    iii. Tanımlanan kurallardan geçen kullanıcılar
    iv. Tanımlanan kurallardan geçemeyen kullanıcılar
    v. Tanımlanan kurallardan geçemeyen kullanıcıların hangi kuraldan/kurallardan dolayı geçemedikleri
    vi. Tarih (gün.ay.yıl) ve zaman (saat:dakika:saniye) bilgisi
    vii. Cihazın MAC ve varsa IP adresi
12) Her bir kurum kullanıcısına Active Directory entegrasyonu ile misafirlere, misafir erişim hakkı vermesi sağlanabilecektir. Ayrıca istenmesi durumunda tanımlanacak sistem yöneticilerine sadece misafir erişim hakkı açma yetkisi verilmiş kullanıcıların açtıkları misafir erişim haklarını izleme, raporlama ve sonlandırma yetkisi sağlanabilecektir.
13) Misafir erişiminin açılması için kullanılacak web sayfasından, ağ erişim kontrol sistemi konfigurasyonlarına kesinlikle ulaşılamayacak. Kurum kullanıcısı sadece misafir kullanıcı açmak için gerekli alanları görebilecektir.
14) Misafir erişimi için misafir kullanıcı bilgileri (misafir kullanıcı adı ve misafir kullanici şifresi), misafire text olarak verilebilecek veya istenmesi durumunda e-mail ile de gönderilebilecektir.

15) Misafir kullanıcılara açılacak erişim hakkı yıl, ay, gün, saat, dakika olarak tanımlanabilecek ve tanımlanan sure sonunda erişim hakkı sistem tarafından otomatik olarak sonlandırılacaktır. Ayrıca, tanımlanan misafir erişim hakkı herhangi bir anda erişim hakkını tanımlayan kullanıcı tarafından sonlandırılabilecektir.
16) Tekli ya da çoklu misafir (aynı anda birden fazla kullanıcı için) erişim hakkı tanımlaması yapılabilecektir.
17) Çoklu erişim hakkı tanımlaması özel olarak hazırlanacak ve kullanıcı bilgilerini içeren bir dosyanın yüklenmesi ile de sağlanabilecektir.
18) Son kullanıcı kişisel bilgisayarlarında aşağıda belirtilen tarama ve kontroller istenmesi halinde ileride lisans ilavesi ile yapılabilecektir.
    i. Microsoft tabanlı İşletim Sisteminin tipi
    ii. Microsoft tabanlı İşletim Sisteminin servis tipi
    iii. Microsoft tabanlı İşletim Sisteminin güncelliği
    iv. Antivirus yazılımının yüklü olup olmadığı
    v. Antivirus yazılımının güncelliği, marka bağımsız olarak versiyon kontrolü yapabilmeli, ilgili antivirus yazılımının bir ay dan daha eski olup olmadığını kontrol edebilmelidir.
    vi. Bilgisayarda o anda çalışmakta olan servisler
    vii. Bilgisayarda o anda çalışmakta olan uygulamalar
    viii. İstenilen uygulamanın o anda çalışıp çalışmadığı
    ix. Bilgisayarın registry (kütük)'sindeki alanlar
    x. Bilgisayarın hard diskindeki dosyalar
19) Teklif edilecek sistem sanallaştırma destekleyebilecektir.
20) Teklif edilecek sistem Secure Syslog destekleyecektir.
21) Teklif edilecek ağ erişim kontrol sistemi çözümü istenmesi durumunda aktif-aktif yedeklilik yapısında çalışabilecektir.
22) Ağ erişim kontrol sistemi, bu teknik şartnamede yapılması istenilen özellikleri içeren lisanslama ile birlikte en az 2000 adet aktif IP için sanal ortamda çalışacak şekilde teklfi edilecektir.
23) Ağ erişim kontrol sistemi üzerindeki tüm lisanslar eş zamanlı bağlantı tipinde çalışacaktır. Bağlantısı kopan veya oturumunu kapatan kullanıcı/endpoint' e ait lisans anında yeni bağlanacak olan kullanıcı/endpoint için kullanılabilir durumda olacaktır.
24) Teklif edilecek sistem en az 3 yıl üretici destek paketi ile teklif edilmelidir.
25) Teklif edilecek çözümün ağda bulunan kenar ve omurga anahtarlar ile aynı marka olması tercih sebebidir.

4. İLERİ MERKEZİ LOG VE OLAY YÖNETİM SİSTEMİ MODÜLÜ (Log Yönetim Çözümü)

1. Sistemin Genel Özellikleri

- Ürün maksimum EPS değerleri şartlara bağlı olmayacaktır. Örneğin default olarak kurulursa desteklediği EPS ile yeni bir filtre tanımlanırsa, yeni bir parser yazılırsa veya yeni kurallar tanımlanırsa desteklediği EPS azalır şeklinde bir kısıtı olmayacaktır.
- Ürün en az 3 yıllık lisans ile teklif edilecektir.
- Maksimum 1000 EPS için 1 TB Diskte logları canlıda en az 365 gün, maksimum 3000 EPS için 3 TB diskte logları en az 365 gün canlıda tutabilmelidir. İki durumda da arşivde 2 yıl tutmalıdır.
- Ürün yedeklerden dönebilmelidir. Sistem log toplamaya devam ederken 60 dakikalık yedeği 30 dakikada geri yüklemeli, eğer log toplamaya devam etmiyorsa 15 dakikada yedeği geri yüklemeyebilmeli.
- Merkezi Log ve Olay Yönetim Sistemi gerektiğinde sanal makinelere kurulabilmelidir.
- Sistem, idaremizde bulunan tüm log ve bilgi üreten sistemlerden log toplayacak şekilde lisanslanmalı ve kurulmalıdır.
- Sistem raporlama, alarm, korelasyon, görselleştirme, veri ilişkilendirme, tehdit istihbaratı özelliklerine sahip olmalıdır.
- Merkezi Log ve Olay Yönetim Sisteminde yönetim ekranı üzerinden farklı yetkilendirmelere yapılabilmelidir. Kullanıcılar yapılan yetkilendirme dahilinde kendileri ile alakalı kayıtlara erişebilmeli, gerçek zamanlı ve geriye dönük sorgulamalar yapabilmelidir.
- Setup dosyalarını kullanarak yapılan kurulum ile her tür ayar geliştirici firmaya ihtiyaç duymadan yapılabilmelidir.
- Geliştirici firmaya bağımlı olmadan programdaki her türlü ayar kurum tarafından ara yüzden yapılabilmelidir.
- Birden fazla firewall ve/veya URL filtre/Proxy loglarını aynı anda sorgulama ve en çok gezilen site, en çok trafik oluşturan makine gibi sorulara bütün hepsini kapsayacak şekilde verilebilmelidir.
- Sistem, güvenlik güncellemeleri, üreticinin kural güncellemeleri, konfigürasyon bilgilerinin girilmesi vb işlemler minimum kullanıcı müdahalesiyle yapılabilmelidir.
- Merkezi Log ve Olay Yönetim Sistemi Windows a setup dosyası kurulmalıdır.
- Sistem ihtiyaç duyduğu veritabanı ve/veya web sunucu gibi üçüncü parti yazılımları kendisi setup ile birlikte otomatik kurup ayarlarını otomatik yapabilmelidir.
- Merkezi Log ve Olay Yönetim Sisteminin backdoor ve casus yazılımlar için güvenlik testlerinin yapılmış olması gerekmektedir.
- Merkezi Log ve Olay Yönetim Sistemi yazılımının WEB tabanlı arayüzü olmalıdır.
- Merkezi Log ve Olay Yönetim Sistemi yazılımında çoklu kullanıcı ve yetkilendirme desteği ile aynı anda en az 10 farklı kullanıcı grubu oluşturulabilmelidir.
- Sistemin diğer bileşenlere bağımlı olmayan ayrı bir korelasyon motoru olmalı ve korelasyon loğlar disk yazılmadan önce hafızada yapılmalıdır.
- Sistemin anlık-gerçek zamanlı(real-time) çalışabilmesi, yükse kapasitedeki veriyi işleyebilmesi, anlık tepkimelere çok hızlı cevap verebilmesi için Merkezi Log ve Olay Yönetim Sistemi

korelasyon kurallarını RAM düzeyinde işlemeli "in memory " çalışmalıdır. Korelasyon kurallarının üzerinde işletilecek "yakın zamanlı loglar" veritabanına yazılmadan önce memory'de tutulmalı, burada işlenmeli ve korelasyon kuralları buradan alarm ürettirmelidir.

- Yazılım 5651 sayılı yasaya uygun olarak zaman damgası ile logları damgalayabilmelidir.
- Sistemin tüm menüleri ve menü içindeki önemli fonksiyonlar kullanıcı bazlı yetkilendirilebilecektir. Böylelikle kullanıcılar sadece kendilerine özel menüleri görebilecek ve sistem üzerinde kendilerine verilen kadar yetkiye sahip olacaklardır.
- Tüm raporlar kullanıcı group yada profillleri bazlı yetkilendirilebilecektir. Raporlama kullanıcıları sadece kendilerine ait raporları görebilecektir.

2. Log Toplama ve Yönetim Sistemi

- Birden fazla porttan SYSLOG ve SNMP TRAP dinleyebilmelidir. Mesela 514, 515 ve 1514 den SYSLOG dinleyip 162 ve 1162 den de SNMP Trap dinleyebilmelidir. Bütün bu ayarlamalar web ara yüzünden yapılabilmelidir.
- Logları konsolide edebilmeli. Örnek; 2 farklı marka ve model firewalldan gelen logları tek bir rapor ekranında gösterebilmelidir.
- Ajanlı veya ajansız log toplamayı desteklemelidir.
- DHCP loglarını herhangi bir MAC adresi bir IP yi ne zaman almış ve ne zaman bırakmış şeklinde raporlayabilmelidir.
- Arayüzde her bir log kaynağından ayrı ayrı ne kadar log geldiği anlık olarak gözükmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, log imzalamayı kayıt geldiği anda yapmalıdır.
- Merkezi Log ve Olay Yönetim Sistemi; SNMP Trap, SNMP, SYSLLOG, Text Dosya Takibi modunda çalışabilecektir.
- SYSLOG, SNMP ve SNMPTRAP protokolünde birden fazla ve farklı farklı port tanımlanabilmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, SYSLOG paketleri ve SNMP Paketlerini kendisi toplayabilmelidir. Eğer üçüncü parti bir yazılım kullanıyorsa bu yazılımların Windows, Linux ve Solaris için de var olduğunu beyan etmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, arayüz ve arayüzle ilişkili servislerden birinin herhangi bir sebepten durması, bozulması veya çalışmaması durumunda log toplamaya devam etmelidir.
- Sistem web arayüzü ve/veya web sunucunun herhangi bir sebepten dolayı çalışmaması durumunda log toplamaya devam edebilmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, log toplanacak bir sistemden (firewall,UTM vs..) kullanıcı tarafından belirlenen süre içinde log almazsa yetkili olarak belirlenmiş kişiyi e-mail ile uyarabilmelidir.

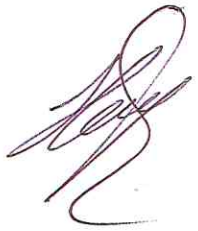
3. Disk Yönetimi

- Sistem logları canlı arama için de sıkıştırılmış olarak tutacaktır
- Sıkıştırılmış loglar ve indexler üzerinden canlı arama yapılabilecektir.
- Indexler de sıkıştırılacak ve sıkıştırılmış indexler üzerinden de canlı arama yapılacaktır
- Sistem index kullanmadan da hızlı ve arayüzden hızlı arama yapabilecektir.
- Canlı arama için kullanılan loglar ve indexleri 1:20 oranında sıkıştırılacaktır.

4. Arama, Raporlama ve Dashboard Sistemi

- Firewall raporlarında paket boyutuna göre büyüktür, küçüktür, eşittir gibi filtreler uygulanabilmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, farklı kaynaklardan toplanan logları belirli bir zaman aralığına ve parametrelere göre arayüz üzerinden sorgulayabilmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, sistemde log toplama desteği verilen cihazlar için en çok gezilen siteler,en çok interneti kullanan cihazlar, en yoğun trafik oluşturan cihazlar vs.. gibi detay raporları sağlayabilmelidir.
- Merkezi Log ve Olay Yönetim Sisteminın Raporlama modülü olmalıdır ve aşağıda tanımlanan hazır raporları sağlamalıdır.
  - Windows İşletim Sistemi Raporları
  - Linux İşletim Sistemi Raporları
  - Cisco Sistem Raporları
  - Sanal Makineler Raporları
  - Güvenlik Raporları
  - Trafik Raporları
  - Firewall Raporları
  - Mail Sunucu Raporları
  - Veritabanı Raporları
  - Web Server Raporları
  - VPN Raporları
  - Web Erişimleri Raporları

- Merkezi Log ve Olay Yönetim Sistemi, Windows event logları üzerinden logon olayları, logon olayları üzerinden filtre ve raporlar hazırlayabilmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, Windows event logları üzerinden dosya erişim raporları hazırlayabilmelidir.
- Sistemde rapor hazırlama sihirbazı olmalıdır.
- Sistemde sınırsız sayıda raporlama kullanıcısı tanımlanabilmelidir.
- Raporlama kullanıcıları istenen raporlar sadece kullanıcılar ile ilgili bölümleri içerecek şekilde atanabilmelidir.
- Sistemde WEB arayüzünden erişilen tüm raporlar için tüm kolonlar ile filtreleme ve arama yapmayı desteklemelidir.
- Sistemde PDF ve CSV rapor çıktılarını desteklemelidir.
- Sistem, topladığı loglar içinde tüm kolon isimleri veya değerler için AND, OR, NOT, include, group by belirli değerler içinde gruplama, sayısal değerler içinde aralık verebilme, IP değerleri içinde aralık verebilme gibi mantıksal kriterler ile arama yapabilmelidir. Kullanımı ve esnekliği kolay olmalı ve öğrenilebilir olmalıdır. Dolayısı ile script, yazılım dili yada arama dili ile sağlanması gibi özelliklere yer verilmemelidir.
- Oluşturulan dashboardlar arası belirli kurallar ile otomatik geçiş yapabilecek görüntüleme ve operasyon merkezi özellikleri olmalıdır.



5. Analiz, İlişkilendirme ve Görselleştirme

- Kullanıcı kendi menülerini ve bu menülerin altlarında kendi raporlarını tasarlayabilmelidir.
- Merkezi Log ve Olay Yönetim Sistemi, GUI bir gösterge paneline (dashboard) sahip olmalıdır. LOG yönetim sunucusunun çalışma durumu, diskteki boş alan durumu gibi sistemin çalışmasını etkileyebilecek parametrelerin anlık olarak takip edildiği bir bölüm panel üzerinde yer almalıdır.
- Merkezi Log ve Olay Yönetim Sistemi; Ağ trafik bilgilerine, kaynak ve hedef IP adresine, seçilen port'a veya belirlenen zaman gibi kriterlere göre sorgulama yapmalıdır.
- Sistem üzerinde güvenlik olaylarının detaylı analizi, veri analizi ve görselleştirme için özel bir platform sunulacaktır.
- Sistem topladığı tüm loglar, tüm kolonlar ve değerleri için analizi kolaylaştıracak özel uygulama ve analiz ortamı sunacaktır.
- Bütün network aktivitelerin eksiksiz olarak ekrandan takip edebilecektir. Örnek olarak son 1 saate oluşan bütün aktiviteler
    - Logon hareketleri
    - Şüpheli hareketler
    - Firewall tarafından izin verilen trafik
    - Firewall tarafından bloklanan trafik
    - Başarısız oturum açma hareketleri
    - Spam trafiği Vb.

- Hazır korelasyon kütüphanesinde en az 150 hazır kural olacaktır.
- Log kaynakları tanımlanırken yapılan isimlendirme aynen raporlara yansımalı ve bu isimlendirmeler ile arama yapılabilmeli.

6. Tehdit İstihbaratı

- Merkezi Log ve Olay Yönetim Sistemi, en az 60 farklı kaynaktan tehdit istihbaratı alıp en az 800 000 tekil IP/URL/Domain den oluşan bir tehdit istihbaratı takip listesini gerçek zamanlı olarak bu verileri IP, URL ve DNS logları ile korelasyona sokulabilmelidir. Bu istihbarat listesindeki bir IP/URL/DNS den veya IP/URL/DNS ye trafik olursa anında (max 15 saniye içinde) uyarı üretebilmelidir.
- Toplan tehdit istihbaratı kaynakları yönetilebilir olmalı, hangi kaynaklardan veri toplandığı ara yüzden takip edilebilmeli ve gerçek zamanlı olarak kaynakların içerdiği IP/URL listesi ekrandan görüntülenebilmeli
- Tehdit istihbarat kaynakları yönetilebilir olmalı. İstenen kaynak listeden çıkarılabilmeli ve yeni kaynaklar da listeye eklenebilmeli ve bütün bu işlemler ara yüzden yapılabilmeli.
- Tehdit istihbaratı verileri korelasyon için kullanılabilmeli.

5. DESTEK HİZMET PAKETİ

1. Telefon ile acil bildirimlerde en geç 30 dk içerisinde uzaktan erişim ile müdahale edilmeli.
2. E-posta veya kayıt yolu ile açılan bildirimlere maksimum 1 saat içerisinde müdahale edilmeli.
3. Firma yetkilisine 7 gün x 24 saat ulaşılabilir durumda olunmalı ve çağrılara en geç 1 saat içerisin de dönüş yapılmalıdır.
4. Bakım, güncelleme ve acil olmayan bildirimlerde maksimum 24 saat içerisinde müdahale edilmelidir.
5. Fiziki müdahale gerektiren acil durumlarda en geç 4 saat içerisinde müdahale edilmeli ve yaşanabilecek olağan dışı durumlarda cihaz değişimi için yedek cihazın konumlandırılabilecek durumda olunması gerekir.
6. Destek paketi süresi 3 yıl olacaktır.

Hayriye Gürsoy
Bilgi İşlem Md.