TEKNİK ŞARTNAME

24 PORT SWİTCH TEKNİKŞARTNAME

1) Kenar anahtar omurga anahtar ile aynı üreticininin ürünü olacaktır.
2) Anahtar üzerinde 24 adet 10/100/1000BaseT Gigabit Ethernet portu ve 4 adet 1G/10G SFP+ ethernet olmak üzere aynı anda çalışabilen toplam 28 adet aktif port'a sahip olmalıdır. SFP Port'lar üzerinde 1000BaseSX , 1000BaseLX SFP, 10GBASE-SR, 10GBASE-LR SFP Modül'ler takılabilmelidir.
3) Anahtar en az 256 Gbps switching kapasitesine ve 96 Mpps paket iletim kapasitesine sahip olmalıdır.
4) Anahtar; IEEE 802.3af PoE ve 802.3at PoE+ ve 802.3bt HPoE protokollerini desteklemelidir. Toplam 370 watt PoE değerine sahip olmalıdır. Anahtar IEEE 802.3 10BaseT, IEEE 802.3u 100BaseTX, IEEE 802.3ab 1000BaseT, IEEE 802.3z 1000BaseX, özelliklerine sahip olacaktır.
5) Teklif edilecek anahtara ait tüm 1000BaseT Port'lar Auto-sense (karşı port hızını tanıma) ve Auto-uplink destekli olmalıdır.
6) Anahtar; web tabanlı olarak konfigüre edilip yönetilebilmelidir. Aynı zamanda; Telnet, SSH ile komut satırından yönetilebilmelidir. SSL, SSH v1,v2 destekli olmalıdır. Switch yazılımları (Firmware) web arayüzden veya FTP üzerinden güncellenebilmelidir.
7) Anahtar üzerinde port ve hız değerlerini gösteren LED'ler olmalıdır.
8) Anahtar 16,000 adet MAC adres tablosuna sahip olmalıdır.
9) Anahtar IEEE 802.1D Spanning Tree Protocol(STP), IEEE 802.3w Rapid Spanning Tree Protocol(RSTP) IEEE 802.1s Multiple Spanning Tree Protocol(MSTP), protokollerini desteklemelidir. Anahtar ayrıca IEEE802.1d STP, IEEE802.1w RSTP, standard 802.1s MSTP, Port fast, BPDU filter, BPDU guard, TC guard, TC protection, ROOT guard protokollerini desteklemelidir.
10) Anahtar üzerinde oluşabilecek lopları önlemeye yönelik özelliğe sahip olmalıdır.
11) Anahtar üzerindeki tüm portlar için sekiz adet önceliklendirme sırası tanımlanabilmelidir.
12) Anahtar; IEEE 802.1AB LLDP/LLDP-MED protokollerini desteklemelidir.
13) Anahtar 802.1Q standardını sağlamalıdır; port, protokol, IP subnet, MAC tabanlı 4K VLAN desteği olmalıdır.
14) Anahtar Voice VLAN ve GVRP protokollerini desteklemelidir.
15) Anahtar DHCP server, DHCP client, DHCP snooping, DHCP relay, IPv6 DHCP snooping, IPv6 DHCP client, IPv6 DHCP relay ozelliklerine sahip olmalidir.
16) Anahtar; L2/L3/L4 Access Control List (ACL) IPv4 ve IPv6 destekli olmalıdır. MAC adresine göre erişim kontrolü yapabilmelidir. Layer 2 seviyesinde MAC, Layer 3 seviyesinde IP, Layer 4 seviyesinde TCP ve UDP port tabanlı erişim denetim listeleri yazılabilmelidir. Anahtar ToS (Type of Service) DSCP işaretleme desteğine sahip olmalı ve QoS hizmeti DSCP'ye göre yapılabilmelidir.
17) Anahtar RADIUS ve TACACS+ serverları ile entegre çalışabilmelidir. Birden fazla RADIUS ve TACACS+ Server desteği olmalı, kimlik doğrulama ve yetkilendirme işlemlerini yapabilmelidir.
18) Anahtar atak ve saldırılara karşı DHCP Snooping, ARP Inspection, Port Isolation, Source guard, CPU protection gibi özelliklere sahip olmalıdır.
19) Anahtar 802.1p queuing method: SPQ/WRR/WFQ protokollerini desteklemelidir.
20) Anahtar port, ip, protokol ve politika bazlı hız limitlemesi yapabilmelidir.
21) Anahtar multicast paketleri için IGMP v1, v2, v3 Snooping, IGMP filtreleme, MLD Snooping v1, v2 özelliklerine sahip olmalıdır.
22) Anahtar SNMP v1, v2 ve v3 desteklemelidir, en az RMON 1, 2, 3, 9 gruplarını desteklemelidir.

23) Anahtar IEEE 802.3ad Link Aggregation destekli olmalıdır.
24) Anahtar IEEE 802.1x port bazlı erişim denetimi sağlamalıdır.
25) Anahtar DHCP Relay(IPv4, IPv6) ve IPv4 için de DHCP 82 profilleri oluşturulmalıdır.
26) Anahtar Port Mirroring özelliğine sahip olacaktır, IP/TCP/UDP Port Mirroring ve Policy-based Port Mirroring desteklemelidir.
27) Anahtar NTP (Network Time Protocol) desteği ve yaz saati ayarları yapılabilir olmalıdır.
28) Anahtar yapılandırma kolaylığı sağlaması için, bir port'a yapılan konfigurasyon diğer portlara kopyalanabilmelidir.
29) Anahtar uzak sunuculara SYSLOG aracılığı ile kayıtları gönderebilecektir
30) Anahtar 0° ile 50° sıcaklık değerleri ve 10 ile 95 nem değerlerinde çalışmaya uygun olmalıdır.
31) Anahtar MAC, VLAN, Basic QinQ, Felix QinQ, Mirroring, STP, RSTP, MSTP, Broadcast storm control, IGMP v1/v2 snooping, IGMP filter, IGMP fast leave, Jumbo frame, RLDP, LLDP, REUP, G.8032 Layer 2 ozelliklerini desteklemelidir.
32) Anahtar üzerindeki Mini-GBIC Modüller anahtar ile aynı marka olmalıdır. Oem Mini Gbic modüller kabul edilmeyecektir.
33) Anahtar statik routing, RIP, RIPng yonlendirme protokollerini desteklemelidir.
34) Anahtar en az 500 adet Ipv4/Ipv6 yonlendirme tablosuna sahip olmalidir.
35) Anahtar en az 500 adet ACL (Access Control List) yazilmasini desteklemelidir.
36) Anahtar ile ücretsiz kurulum yazılımı da teslim edilmelidir. Kurulum yazılımı IP bağımsız olarak networkte bulunan anahtarlar listelenebilmelidir.

48 PORT SWİTCH TEKNİKŞARTNAME

1. Anahtar üzerinde 48 adet 10/100/1000BaseT Gigabit Ethernet portu ve en az 4 adet 1G/10G Base-X SFP+ ethernet portu bulunmalıdır. Aynı anda 52 adet port aktif olarak çalışabilmelidir.
2. Anahtar en az 264 Gbps switching kapasitesine ve 132 Mpps paket iletim kapasitesine sahip olmalıdır.
3. 3. Anahtar IEEE 802.3 10BaseT, IEEE 802.3u 100BaseTX, IEEE 802.3ab 1000BaseT, IEEE 802.3z 1000BaseX, özelliklerine sahip olacaktır.
4. 6. Anahtar 9 adete kadar yığınlanabilir ve tek bir IP adresi üzerinden yığın yönetilebilir olmalıdır. Anahtarlar tek bir yönetim paneline sahip olmalı, yığın içerisinde farklı portlardan port gruplaması yapılabilmelidir. Yığın içerisinde PoE ve PoE olmayan anahtarlar yer alabilmelidir
5. Anahtar statik routing, RIP ve RIPng yönlendirme protokollerini desteklemelidir
6. Teklif edilecek anahtara ait tüm 1000BaseT Port'lar Auto-sense (karşı port hızını tanıma) ve Auto-uplink destekli olmalıdır
7. Anahtar; web tabanlı olarak konfigüre edilip yönetilebilmelidir. Telnet, SSH ile komut satırından yönetilebilmelidir. SSL, SSH v1,v2 destekli olmalıdır. Switch yazılımları (Firmware) web arayüzden veya FTP üzerinden güncellenebilmelidir.
8. Anahtar en az 500 adet Ipv4/Ipv6 yönlendirme tablosuna sahip olmalidir.
9. Anahtar en az 500 adet ACL (Access Control List) yazilmasini desteklemeli
10. Anahtar IEEE 802.1d Spanning Tree Protocol (STP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) veya benzer protokolleri desteklemelidir
11. Anahtarın güç kaynakları 1+1 modüler olarak yedeklenebilir ve çalışma esnasında sökülüp takılabilir (hot-swappable) yapıda olmalıdır. Cihazın çalışmasının ve yedeklilliğini sağlayacak güç üniteleri ile birlikte teklif edilmelidir

12. Anahtar SNMP v1, v2 ve v3 desteklemelidir, en az RMON 1, 2, 3, 9 gruplarını desteklemelidir.
13. Anahtar IEEE 802.3ad Link Aggregation destekli olmalıdır.
14. Anahtar IEEE 802.1x MAB ve web portal tabanlı kimlik denetimi sağlamalıdır.
15. Teklif edilecek cihaz, SDN (Software Defined Networking) destekleyebilen (hazır ve uyumlu) bir cihaz olmalıdır. Cihaz Openstack veya OpenFlow 1.3 özelliğini destekleyebilecektir. Bu sayede cihaz API (Application Programming Interface)'leri, Açık Kaynak Kodlu Arayüzler ve Scripting dilleri kullanılarak cihaz üzerinde yönetimsel kararlar alınabilecektir
16. Anahtar NTP ve SNTP özelliklerine sahip olmalıdır.
17. Anahtar IEEE 802.1x MAB ve web portal tabanlı kimlik denetimi sağlamalıdır
18. Anahtar Port Mirroring özelliğine sahip olacaktır, birden fazla portu tek bir porta, tek portu birden fazla porta aynalayabilmelidir
19. Anahtar atak ve saldırılara karşı DHCP Snooping, ARP Inspection, Port Protection, Source guard, CPU protection güvenlik özelliklere sahip olmalıdır
20. 26. Anahtar 802.1x RADIUS ve TACACS+ serverları ile entegre çalışabilmelidir. Birden fazla RADIUS ve TACACS+ Server desteği olmalı, kimlik doğrulama ve yetkilendirme işlemlerini yapabilmelidir. Üretici özel yetkilendirme protokolleri kullanılmayacaktır
21. Anahtar uzak sunuculara SYSLOG aracılığı ile kayıtları gönderebilecektir.
22. Anahtar üzerindeki Mini-GBIC Modüller anahtar ile aynı marka olmalıdır. Oem Mini Gbic modüller kabul edilmeyecektir
23. Anahtar akıllı fan yapısına sahip olmalıdır.
24. Anahtar 0° ile 50° C° sıcaklık değerleri ve %10 ile %90 bağıl nem değerlerinde çalışmaya uygun olmalıdır.
25. Anahtar Voice VLAN ve GVRP protokollerini desteklemelidir.
26. Anahtar en az 4094 adet 802.1q VLAN ID desteklemelidir.
27. Anahtar DHCP server, DHCP client, DHCP snooping, DHCP relay, IPv6 DHCP snooping, IPv6 DHCP client, IPv6 DHCP relay, DHCP Opsiyon 82 özelliklerine sahip olmalidir.
28. Anahtar; L2/L3/L4 Access Control List (ACL) IPv4 ve IPv6 destekli olmalıdır. MAC adresine göre erişim kontrolü yapabilmelidir. Layer 2 seviyesinde MAC, Layer 3 seviyesinde IP, Layer 4 seviyesinde TCP ve UDP port tabanlı erişim denetim listeleri yazılabilmelidir. Anahtar ToS (Type of Service) DSCP işaretleme desteğine sahip olmalı ve QoS hizmeti DSCP'ye göre yapılabilmelidir
29. Anahtar montajı yapılacak ortamın olumsuz şartlarından etkilenmeyecek, korozyon korumasına sağlayan Conformal Coating uygulamasına sahip olmalıdır. Anahtar ilgili conformal coating testlerine ve sertifikalarına sahip olmalıdır.
30. Anahtar NTP ve SNTP özelliklerine sahip olmalıdır.
31. Anahtar yönetim amaçlı SDN özelliklerini OpenFlow desteğine sahip olmalıdır.
32. Anahtar en az 4KV şimşek koruması sağlamalıdır
33. Anahtar 8 adet donanım tabanlı öncelik kuyruğu bulunacaktır.
34. Anahtar Port fast, BPDU filter, BPDU guard, TC guard, TC protection, ROOT guard protokollerini desteklemelidir
35. EoS (End of Sale) ve EoL (End of Life) duyuruları yapılmamış ve üreticinin web sitesinde yer alıyor olmalıdır.
36. Anahtar en az 5 yıl üretici garantili olmalı. Eğer üretici tarafından 5yıl garanti karşılanmıyorsa dağıtcı veya yüklenici tarafından 5yıl garanti ile teklif edilmelidir

FİBER DAĞITM ve OMURGA AĞ ANAHTARI

1) Anahtar, en az 20 adet 1G/10G SFP portu, en az 4 adet 10G/25G SFP28 ve en az 2 adet 40G QSFP+ port olmak üzere en az 26 adet aktif porta sahip olmalıdır.
2) Anahtar üzerinde yönetim amaçlı bir (1) adet RJ-45 ethernet out of band management portu, 1 adet RJ45 tipinde RS232 konsol portu ve bir (1) adet USB konsol portu bulunmalıdır.
3) Anahtar en az 2560 Gbps switching kapasitesine ve 570 Mpps paket iletim kapasitesine sahip olmalıdır.
4) Anahtar en az 4000 adet VLAN desteğine sahip olmalıdır.
5) Anahtar; Port-based VLAN, Private VLAN, Super VLAN, QinQ ve GVRP özelliklerine sahip olmalıdır.
6) Anahtar IEEE 802.3ad Link Aggregation ve LACP özelliklerini desteklemelidir.
7) Anahtar Port Mirroring özelliğine sahip olacaktır, birden fazla port tek bir port üzerinden izlenebilmeli ve birden fazla anahtar üzerinde izlenebilmelidir. Anahtar RSPAN özelliklerini desteklemelidir.
8) Anahtar IEEE 802.1D Spanning Tree Protocol(STP), IEEE 802.1w Rapid Spanning Tree Protocol(RSTP) IEEE 802.1s Multiple Spanning Tree Protocol(MSTP), protokollerini desteklemelidir.
9) Anahtar Layer 3 özelliklerine sahip olmalı, statik routing, RIP, OSPFv2, BGP4, IS-ISv4 IPv4 yönlendirme protokollerini desteklemelidir. Bu protokoller lisanslı ise lisansları ile teklif edilmelidir.
10) Anahtar Layer 3 özelliklerine sahip olmalı, IPv6 statik routing, RIPng, OSPFv3, BGP4+, IS-ISv6 IPv6 yönlendirme protokollerini desteklemelidir. Bu protokoller lisanslı ise lisansları ile teklif edilmelidir.
11) Anahtar Layer 3 ECMP yönlendirme özelliğine sahip olmalıdır.
12) Anahtar VRRP özelliklerine sahip olmalıdır.
13) Anahtar, IGMPv1/v2/v3, IGMPv1/v2/v3 Snooping, MLD Snooping, PIM-DM, PIM-SM, PIM-SSM, MSDP, Multicast protokollerini desteklemelidir.
14) Anahtar üzerinde IPv6 için erişim denetim listesi (ACL) yazılabilmelidir.
15) Anahtar RADIUS ve TACACS+ kimlik doğrulama yapabilecektir. Anahtarı yönetecek kişiler hiyerarşik olarak erişimleri sağlanabilecektir.
16) Anahtar; L2/L3/L4 Access Control List (ACL) IPv4 ve IPv6 destekli olmalıdır. MAC adresine göre erişim kontrolü yapabilmelidir. Layer 2 seviyesinde MAC, Layer 3 seviyesinde IP, Layer 4 seviyesinde TCP ve UDP port tabanlı erişim denetim listeleri yazılabilmelidir ACL80 desteklemelidir. Anahtar 801.1p, ToS (Type of Service) DSCP işaretleme desteğine sahip olmalı ve QoS hizmeti DSCP'ye göre yapılabilmelidir.
17) Anahtar SP, WRR, DRR, SP+ WRR, SP+DRR, RED/WRED kuyruk planlamasını desteklemelidir.
18) Anahtar DHCP server, DHCP client, DHCP relay, IPv6 DHCP client, IPv6 DHCP relay ozelliklerine sahip olmalidir.
19) Anahtar SNMP, CLI (Telnet/Konsol), SSH, RMON 1, 2, 4, 9 gruplarını desteklemelidir. NTP, Ipv6 SNMP, Ipv6 SNMP MIB desteği, Telnet V6, FTP/TFTP v6, DNS v6, NTP v6, Traceroute v6 desteklemelidir.
20) Anahtar yığınlanabilir mimaride olmalıdır.
21) Anahtar uzak sunuculara SYSLOG aracılığı ile kayıtları gönderebilecektir.
22) Anahtar SFlow desteğine sahip olmalıdır.

23) SFP+ Portlara 10GBASE-LR, 10GBASE-SR, 10GBASE-ER, 1000BASE-LX/LH, 1000BASE-SX, 1000BASE-BX ve 1000BASE-ZX, QSFP+ portlara 40G-QSFP-SR, 40G-QSFP-LR4 modüller takılabilmelidir.
24) Anahtarın güç kaynakları dahili olarak yedeklenebilir ve çalışma esnasında sökülüp takılabilir (hot-swappable) yapıda olmalıdır. Anahtar ile birlikte en az 2 adet Güç kaynağı takılı olarak teslim edilecektir. Güç kaynaklarının girişi 100VAC ile 240VAC aralığını desteklemelidir.
25) Anahtar üzerindeki fanlar yedekli çalışmalıdır. Anahtar üzerinde yedekli çalışabilecek en az 2 adet fan olmalıdır.
26) Anahtar 0°C ile 50°C ortam sıcaklığında ve %10 ile %90 yoğuşmasız nem aralığında çalışabilmelidir.
27) Anahtar üzerindeki SFP Modüller anahtar ile aynı marka olmalıdır. Oem SFP modüller kabul edilmeyecektir.
28) Anahtar, CE sertifikasına sahip olacaktır.
29) Anahtar en az 3 yıl üretici garantisine sahip olmalıdır.

BİRLEŞİK TEHDİT YÖNETİMİ CİHAZI

Mimari

1,1 Ürün ICSA Network Firewall Sertifikasına sahip olmalıdır.
1,2 OEM yerel satış ve destek birimine sahip olmalıdır.
1,3 Önerilen cihaz çok işlevli LCD ekrana sahip olmalıdır.
1,4 Önerilen cihaz kütük ve raporların saklanması için dahili bir sabit diske sahip olmalıdır.
1,5 Önerilen çözüm FCC ve CE normlarına uymalıdır
1,6 Önerilen çözüm aşağıdaki kıstaslara uymalıdır.
a. 64 bitlik donanım platformuna sahip olmalıdır
b. Çok çekirdekli paralel işlemci mimarisi tabanlı olmalıdır
c. 8 adet 10/100/1000 mbps Ethernet portu olmalıdır. 2 adet GbE management porta sahip olmalıdır. En az 6 adet Flexi Port yuvası bulunmalıdır.
d. Saniyede 220.000 yeni oturumu desteklemelidir.
e. 30.000.000 eşzamanlı oturumu desteklemedir.
f. Güvenlik Duvarı kapasitesi 85 Gbps olmalıdır.
g. VPN kapasitesi 9 Gbps olmalıdır.
h. IPS kapasitesi 20 Gbps olmalıdır.
i. NGFW kapasitesi 18 Gbps olmalıdır.
j. Anti virüs kapasitesi 13 Gbps olmalıdır.
k. 2 adet USB 2.0 ve 1 adet USB 3.0 porta sahip olmalıdır.
1,7 Önerilen cihaz sınırsız kullanıcı/nokta lisansına sahip olmalıdır.
1,8 Önerilen çözüm tek başına dahili firewall'a sahip HTTP proxy (vekil) sunucusu, Antivirüs, içerik filtreleme ve IPS olarak çalışabilmelidir.
1,9 Önerilen çözüm güvenlik ve internet yönetimi için kullanıcı tabanlı politika yönetimini desteklemelidir.
1,10 Önerilen çözüm sadece IP adresine göre değil kullanıcı isimlerine göre de cihaz üzerinde raporlamayı desteklemelidir.
1.11 Önerilen cihazın 48 GB hafızası olmalıdır.

1,12 Önerilen cihaz 2U Raf tipi montajlı olmalıdır.
1,13 Önerilen cihazın en az 2x480 GB SSD diski olmalıdır.
1,14 Önerilen cihaz CB, CE, FCC Sınıf A, VCCI, CTick, UL, CCC sertifikalarına sahip olmalıdır.
1,15 Önerilen çözüm, dahili otomatik kademeli 110-240VAC, 50-60 Hz güç kaynağına sahip olmalıdır.
1,16 Önerilen çözüm, desteklenen Access Pointler ile Voucher, günlük şifre veya Terms of Acceptance modları ile Hotspot yapılandırmasına izin vermelidir.
1,17 Önerilen çözüm, desteklenen Access Pointleri ek donanıma ihtiyaç duymadan yönetebilmelidir.

Yönetim, Kimlik denetimi & Genel Konfigürasyon

2,1 Önerilen çözüm HTTPS, SSH ve Konsol üzerinden güvenli bağlantıyla yönetimi desteklemelidir.
2,2 Önerilen çözüm SMS ile Misafir Kullanıcı yetkilendirmesine sahip olmalıdır.
2,3 Önerilen çözüm kullanıcı nesneleri de dahil olmak üzere konfigürasyon yedeklerini yaratıp geri yükleyebilmelidir.
2,4 Önerilen çözüm 3. katmanda veya transparan modda (2. Katman) ayrı ve eşzamanlı olarak kurulabilmelidir.
2,5 Önerilen çözüm kimlik denetimi için Windows NTLM, Active Directory, LDAP, Radius ve RSA SecureID, Novell e-dizin, TACACS+ ya da yerel veri tabanlarını desteklemelidir.
2,6 Önerilen çözüm kimlik denetimi için otomatik tekil girişi desteklemelidir. SSO proxy (vekil) sunucudan bağımsız olmalı ve yetkilendirme için tüm uygulamaları desteklemelidir.
2,7 Önerilen çözüm dinamik DNS servislerini desteklemelidir.
2,8 Önerilen çözüm günlük, haftalık, aylık, ya da yıllık bazda, toplam yada İnternet Servis sağlayıcısına özel bağlantının bant genişliği kullanım grafiğini gösterebilmelidir.
2,9 Önerilen çözüm bağımsız kullanıcı/IP/uygulama aracılığıyla gerçek zamanlı veri transferi/bant genişliği kullanımı sağlamalıdır.
2,10 Önerilen çözüm IP/FQDN ile ana proxy (vekil) sunucu kullanımını desteklemelidir.
2,11 Önerilen çözüm NTP'yi desteklemelidir.
2,12 Önerilen çözüm güvenlik sebebiyle kullanıcı adı/IP/MAC aracılığıyla belli bir IP ve MAC adresindeki kullanıcıyı yönlendirebilmelidir.
2,13 Önerilen çözüm Web yönetim ara yüzünde çoklu dil desteği sağlamalıdır. (İngilizce, Fransızca, Hintçe)
2,14 Önerilen çözüm eski sürümlere geri dönmeyi desteklemelidir.
2,15 Önerilen çözüm oturumun zaman aşımına uğraması ve boşta kalması durumunda kullanıcıları sistemden çıkartmalıdır.
2,16 Önerilen çözüm yönetilebilirlik açısından ACL(giriş kontrol sistemi) tabanlı kullanıcı yaratılmasını desteklemelidir.
2,17 Önerilen çözüm cihaz köprüleme modundayken(Bridge Mode) yerel ağ bypass imkanı sunmalıdır.
2,18 Önerilen çözüm dahili PPPoE istemcisine sahip olmalıdır ve PPPoE her değiştiğinde tüm gerekli bilgileri otomatik güncelleyebilmelidir.
2,19 Önerilen çözüm SNMP v1, v2c'yi desteklemelidir. Netflow desteği bulunmalıdır.
2,20 Önerilen çözüm yazılıma ilişik olmaktan ziyade firmware tabanlı olmalıdır. Cihaz üzerinde eşzamanlı olarak iki yazılımı tutabilmeli ve anında yedeğe geri dönebilmelidir.
2,21 Önerilen çözüm esnek, modüler rol tabanlı ara yüz yönetimine sahip olmalıdır.

2,22 Önerilen çözüm her modül için (örn. Firewall, Farklı VPN türleri) çoklu yetkilendirme sunucularını desteklemelidir.
2,23 Önerilen çözüm çoklu Thin Client (İstemcisi) (Microsoft TSE, Citrix) yetkilendirmesini desteklemeli ve aynı IP adresinden bağlanan kullanıcıları ayırt edebilmelidir.
2,24 Önerilen çözüm aşağıdakileri desteklemelidir:

1. DHCP Sunucusu
2. DHCP Tekrarlama Aracısı
3. Ipsec VPN üzerinden DHCP desteği

2,25 Önerilen çözüm DNS proxy (vekil) sunucu olarak çalışabilmelidir.
2,26 Önerilen çözüm özelleştirilebilir giriş güvenlik ayarlarına sahip olmalıdır.
2,27 Önerilen çözüm özelleştirilebilir "yönetici şifre zorluk ayarlarına" sahip olmalıdır.
2,228 Önerilen çözüm 2-Factor Authentication desteklemelidir.

Çoklu ISP yük dengelenmesi ve çoklu bağlantı

3,1 Önerilen çözüm en az 2 ISP için yük dengeleme ve çoklu bağlantı desteklemelidir.
3,2 Önerilen çözüm, Kaynak, Hedef, Kullanıcı adı ve uygulamayı esas alarak "Explicit Routing" desteklemelidir.
3,3 Önerilen çözüm yük dengelenmesi için ağırlıklı “Round Robin” algoritmasını desteklemelidir.
3,4 Önerilen çözüm ICMP, TCP ya da UDP protokolündeki hata alan ISP bağlantısını algılayabilen arıza giderme şartlarını sağlamalıdır.
3,5 Önerilen çözüm ağ geçidinde bir değişiklik olduğu zaman sistem yöneticisine e-posta göndermelidir.
3,6 Önerilen çözüm aktif/aktif (Round Robin) ve aktif/pasif ağ geçidi yük dengelemesi ve çoklu bağlantıyı desteklemelidir.

High Availability- Yüksek Mevcudiyet

4,1 Önerilen çözüm aktif/ aktif ve aktif/pasif geçerliliği desteklemelidir.
4,2 Önerilen çözümdeki Yüksek Mevcudiyet özelliği ICSA sertifikalı olmalıdır.
4,3 Önerilen çözüm cihazın geçerlilik durumunda değişiklik olduğu zaman sistem yöneticisine uyarı göndermelidir.
4,4 İki istemci arasındaki YM trafiği şifreli olmalıdır.
4,5 Önerilen çözüm bağlantı, cihaz ve oturum aksaklıklarını desteklemelidir.
4,6 Önerilen çözüm ağdaki cihazlar arasında manuel ve otomatik senkronizasyonu desteklemelidir.

Güvenlik Duvarı

5,1 Önerilen çözüm istikrarlı bir işletim sistemine sahip olan tek başına çalışabilen bir cihaz olmalıdır.
5,2 Önerilen çözüm ICSA testlerinden geçmiş sertifikalı bir güvenlik duvarına sahip olmalıdır.
5,3 Önerilen çözüm kullanıcı tabanlı bire bir ve dinamik NAT, PAT durumlarını gözlemleyen bir cihaz olmalıdır.
5,4 Önerilen çözüm firewall kuralarında kaynak/hedef IP/alt ağ/grup, hedef port yanında kullanıcı kimliğini de eşleştirmelidir.
5,5 Önerilen çözüm kullanım kolaylığı açısından firewall kurallarında AV/AS, IPS, içerik filtreleme, bant genişliği kontrolü ve politika tabanlı yönlendirme kararları gibi UTM

kurallarının uygulanmasını desteklenmelidir. Ayrıca UTM kontrolleri bölgeler arası trafiğe uygulanabilmelidir.
5,6 Önerilen çözüm kullanıcı tanımlı çoklu bölge güvenlik mimarisini desteklemelidir.
5,7 Önerilen çözüm port ve imza tabanlı uygulama ön tanımlarına sahip olmalı ve port ve protokol numaralarıyla özel uygulama tanımlamalarına olanak sağlamalıdır.
5,8 Önerilen çözüm First Alive, Round Robin, Random,Sticky IP ve TCP ya da ICMP örneklemesi ile sunucu çalışma kontrolü ile arıza giderme gibi farklı yük dengeleme yöntemlerine sahip iç NAT yük dengelemesini desteklemelidir.
5,9 Önerilen çözüm 802.1q VLAN etiketlemeyi desteklemelidir.
5,10 Önerilen çözüm RIP1, RIP2, OSPF, BGP4 tarzında dinamik yönlendirmeyi desteklemelidir
5,11 Önerilen çözüm Jumbo Frame desteklemelidir.
5,12 Önerilen Sistem kontrol panelinde standart şifre değiştirilmediğinde, güvenli olmayan giriş açık olduğunda ve modülün destek süresi dolmaya yaklaştığında uyarı mesajı göstermelidir.
5,13 Önerilen Sistem OSI 2 ila 7.nci katman güvenliğinin sağlanması için MAC Adresi (Fiziksel Adres) tabanlı firewall kurallarını desteklemelidir.
5,14 Önerilen çözüm www.ipv6ready.org adresindeki ilkelere uygun olarak IPv6 protokolüne hazır olmalıdır.
5,15 Önerilen çözüm VPN ve ağ geçidi - yük dengeleme arızalarına karşı USB arayüzünden 3G UMTS, GSM desteklemelidir.
5,16 Önerilen çözüm yöneticinin uygulama bazlı bant genişliği kuralları tanımlamasını sağlayan uygulama bazlı bant genişliği yönetimini desteklemektedir.

IPS

6,1 Önerilen çözüm ICSA sertifikalı olmalıdır.
6,2 Önerilen çözüm imza ve alışılmadık protokol tabanlı Saldırı önleme sistemi olmalıdır.
6,3 Önerilen çözüm veri tabanında 7000'den fazla imzaya sahip olmalıdır.
6,4 Önerilen çözüm özel IPS imzalarının yaratılabilmesine izin vermelidir.
6,5 Önerilen çözüm ara yüz seviyesindeki politikalar yerine farklı alanlar için çoklu IPS politikalarının yaratılmasını desteklemelidir.
6,6 Önerilen çözüm paket gecikmelerinin azalması için IPS kategori/imzalarının devreye alınıp devreden çıkarılmasını desteklemektedir.
6,7 Önerilen çözüm IPS uyarı ve kütüklerinde IP ile beraber kullanıcı adını da belirtmelidir.
6,8 Önerilen çözüm kendini sunucudan otomatik güncellemelidir.
6,9 Önerilen çözüm saldırılar için uyarı oluşturmalıdır
6,10 Önerilen çözüm kritiklik seviyesine göre en önemli uyarılar ve saldırganları, protokole göre de en çok saldırıya uğrayanları gösteren raporları yaratabilmelidir.
6,11 Önerilen çözüm aşağıdaki eylemlerle oturum tabanlı IPS imza kontrolünü desteklemelidir:
a.Oturum sonlandırma: Tüm oturumu, bu oturumdaki trafik bir IPS imzası ile eşleştiğinde sonlandırmak için.
b. Bypass modu: Tüm oturumu, bu oturumdaki trafik bir IPS imzası ile eşleştiğinde baypas etmek için."

Ağ Geçidi Antivirus Yazılımı

7,1 Önerilen çözüm dahili antivirüs yazılımına sahip olmalıdır.
7,2 Önerilen çözüm ICSA testlerinden geçmiş antivirüs/casus yazılım engelleyicisine sahip olmalıdır.
7,3 Önerilen çözüm Mail Transfer Agent veya SMTP Transparan Proxy olarak çalışabilmelidir.
7,4 Önerilen çözüm SMTP, POP3, IMAP, FTP, HTTP HTTPS ve HTTP üzerinden FTP protokollerinin taranmasını desteklemelidir.
7,5 Önerilen çözümün temel virüs imza veri tabanı tam bir virüs ve türevleri listesi içermesinin yanında yemleme (Phishing) ve casus yazılım gibi kötücül yazılımları(Malware) da tanımlamalıdır
7,6 Önerilen çözüm postalara imza ve feragatname ekleyebilmelidir.
7,7 Önerilen çözüm uygulama ve kullanıcı bazlı karantina desteği sağlamalıdır.
7,8 Önerilen çözüm uzantısına göre dinamik ve işletilebilir dosyaları engellemelidir.
7,9 Önerilen çözüm SMTP trafiğindeki bozuk, şüpheli veya korunmuş eklentiler için aşağıdaki eylemleri desteklemelidir.

a. Yok sayma
b. Postayı eklentisiz yerine ulaştırma
c. Postayı orijinal haliyle yerine ulaştırma
d. Yöneticiyi bilgilendirme

7,10 Önerilen çözüm bilgilendirme, karantina ve dosya uzantılarının kontrolünde gönderici/alıcı e-posta adresi/adres grubuna özel politikaları desteklemelidir. Tek bir sabit kural olmamalıdır.
7,11 Önerilen çözüm hem manuel, hem de bir saatten daha kısa aralıklarla imza tanımlarının otomatik güncellenmesini desteklemelidir.
7,12 Önerilen çözüm POP3 ve IMAP trafiğinde virüslü eklentiyi postadan ayırmalı ve alıcı ve yöneticiyi bilgilendirmelidir.
7,13 Önerilen çözüm HTTP trafiğini kullanıcı adı, kaynak/hedef IP adresi ya da URL bazlı olarak düzenli ifadelerle taramalıdır.
7,14 Önerilen çözüm belirtilen bir HTTP trafiğinin isteğe bağlı olarak taranmamasını desteklemelidir.
7,15 Önerilen çözüm HTTP virüs taraması için gerçek ve batch modlarını desteklemelidir.
7,16 Önerilen çözüm kullanıcı adı, IP adresi, gönderici, alıcı ve virüs adı bazlı eskiye dönük raporlamayı desteklemelidir.
7,17 Önerilen çözüm virüsleri %98'in üstünde bir oranda tanımlayabilmelidir.
7,18 Önerilen çözüm, isteğe bağlı olarak çift antivirüs motoru ile tarama yapabilmelidir.
7,19 Önerilen çözüm, ATP korumasına sahip olmalıdır.
7,20 Önerilen çözüm, ilgili firmanın cloud tabanlı antivirüs çözümü ile birlikte çalışabilmeli ve trafik geçişini uç noktaların antivirüs durumuna bağlı olarak kısıtlayabilmelidir.
7,21 Önerilen çözüm, tek yön mesajlaşma için SPX e-mail kriptolama desteklemelidir.
7,22 Önerilen çözüm, OEMLabs tarafından sağlanan PII, PCI, HIPAA ve daha fazlası için önceden paketlenmiş hassas veri tipi bazlı SMTP kuralını desteklemelidir.

Web Filtreleme Çözümü

9,1 Önerilen çözüm ICSA sertifikalı olmalıdır.
9,2 Önerilen çözüm, başka bir yerdeki veri tabanının sürekli sorgulanmasını engellemek için sisteme entegre yerel bir veri tabanına sahip olmalıdır.
9,3 Önerilen çözüm tek başına HTTP proxy (vekil) sunucu olarak çalışabilmelidir.

9,4 Önerilen çözüm 90+ web kategorisine ait 90 milyon+ URL'yi içeren veri tabanına sahip olmalıdır.
9,5 Önerilen çözüm aşağıdaki özelliklere dahilen sahip olmalıdır
a. HTTPS bazlı bağlantıları engelleyebilmelidir
b. Bağlantıları düzenli ifadeler aracılığıyla engelleyebilmelidir
c. Düzenli ifade tabanlı istisnalar listesine sahip olmalıdır
d. HTTP / HTTPS karşıya gönderim trafiğini engelleyebilmelidir
e. Kategori tabanlı olarak google'ın önbelleğindeki sayfaları engelleyebilmelidir
f. Akamai tarafından sağlanan siteleri engelleyebilmelidir
g. Kullanıcı adı ve IP adresi bazında proxy (vekil) sunucu dışından gelen istekleri tanımlayabilmeli ve engelleyebilmelidir
h. Bağlantı çeviri isteklerini tanımlayabilmeli ve engelleyebilmelidir
9,6 Önerilen çözüm aşağıdaki uygulama engelleme özelliklerini barındırmalıdır
a. Yahoo, MSN, AOL, Google, Rediff, Jabber vb. bilinen sohbet programlarını engelleyebilmelidir.
b. FTP programlarından dosya transferini engelleyebilmelidir.
9,7 Önerilen çözüm internetteki HTTP ve HTTPS tabanlı anonim proxy (vekil) sunucuları engellemelidir.
9,8 Önerilen çözüm her kategori için özel “Erişim Engellendi” mesajı tanımlanmasını desteklemelidir.
9,9 Önerilen çözüm CIPA uyumlu ve CIPA tabanlı ön tanımlı internet erişim kurallarına sahip olmalıdır.
9,10 Önerilen çözüm yönetici tanımlanmasına göre trafiği üretken, etkisiz, sorunlu ve çalışmayan şeklinde sınıflandırabilmelidir.
9,11 Önerilen çözüm web sitelerini geniş olarak sınıflandıran belirli kategorilere sahip olmalıdır. Örneğin çalışanların üretkenliğini azaltan, aşırı bant genişliği kullanan ve zararlı siteler.
9,12 Önerilen çözüm kullanıcı adı, IP adresi, bağlantı, gruplar, kategoriler ve kategori tipleri tabanlı raporlama yapabilmelidir.
9,13 Önerilen çözüm raporlarda uygun verilerin filtrelenmesi için arama yapılmasını desteklemelidir.
9,14 Önerilen çözüm kullanıcı ve grupların günlük/haftalık/aylık/yıllık bazda internet erişimlerini tanımlayan periyodik kuralları desteklemelidir.
9,15 Önerilen çözüm kullanıcı ve grupların internete erişim zamanlarının belirlenmesini desteklemelidir.
9,16 Önerilen çözüm kullanıcı ve grupların günlük/haftalık/aylık/yıllık bazda veri erişimlerini tanımlayan periyodik kuralları desteklemelidir.
9,17 Önerilen çözüm dahili bant genişliği yönetimi kabiliyetine sahip olmalıdır.
9,18 Önerilen çözüm bireysel ya da paylaşmalı bazda her kullanıcı/IP/uygulama için garantilenen ve sağlanabilecek azami bant genişliğini tanımlayabilmelidir.
9,19 Önerilen çözüm kritik uygulamalar için yüksek öncelik seviyelerini desteklemelidir.
9,20 Önerilen çözüm farklı zamanlarda farklı bant genişliği tanımlanmasını desteklemeli ve bant genişliği zamanı geldiğinde otomatik değişmelidir.
9,21 Önerilen çözüm web kategorisi tabanlı bant genişliği yönetimi ve önceliklendirmesi sağlamalıdır.
9,22 Önerilen çözüm Web Caching özelliğine sahip olmalıdır.
9,23 Önerilen çözüm Youtube education filter desteğine sahip olmalıdır.

VPN

10,1 Önerilen çözüm SSL VPN Remote Access için şifreleme yönteminin değiştirilebilmesine izin vermelidir.
10,2 Önerilen çözüm, Site-to-Site ve Remote Access SSL VPN desteklemelidir.
10,3 Önerilen çözüm IPSec (Ağdan ağa, Sunucudan sunucuya, İstemciden siteye), L2TP & PPTP ve SSL VPN bağlantılarını desteklemelidir.
10,4 Önerilen çözüm DES, 3DES, AES, Twofish, Blowfish, Serpent şifreleme algoritmalarını desteklemelidir.
10,5 Önerilen çözüm ön paylaşımlı anahtar ve dijital sertifika bazlı kimlik doğrulamayı desteklemelidir.
10,6 Önerilen çözüm bağlantı kurma sürecinin ilk safhasında ana ve agresif modları desteklemelidir.
10,7 Önerilen çözüm harici sertifikaları desteklemelidir.
10,8 Önerilen çözüm VPN'in uzaktaki bilgisayarlarda rahat kurulumu için "istemciden siteye" bağlantı ayarlarının dışarı verilmesini desteklemelidir.
10,9 Önerilen çözüm standart IPSec VPN istemcilerini desteklemelidir.
10,10 Önerilen çözüm yerel sertifika yetkilerini ve kullanıcı imzalı sertifikaların yaratılması, yenilenmesi ve silinmesini desteklemelidir.
10,11 Önerilen çözüm birden fazla bağlantının gruplandığı VPN arıza giderme yedeklerini desteklemelidir. Bir bağlantı kesildiğinde sistemi bağlı tutmak için otomatik olarak diğer bağlantı etkinleşir.
10,12 Önerilen çözüm arıza giderici VPN yedeği ile otomatik Noktalar Arası Bağlantıyı (MPLS) desteklemelidir.
10,13 Önerilen çözümde verisign/Entrust.net/Microsoft vb. sertifikaları önceden yüklenmiş olmalı ve yeni sertifikaların yüklenmesi desteklenmeli.
10,14 Önerilen çözüm güvenli IPSec/L2TP/PPTP VPN tünellerini desteklemeli.
10,15 Önerilen çözüm Apple iOS ve Android VPN istemcilerini desteklemelidir
10,16 Önerilen çözüm cihaz üzerinde web erişimli (istemci olmadan), Web Uygulama Erişimi (en sık kullanılan protokoller), Tam Tünel (Full Tunnel) ve Ayrık Tünel (Split Tunnel) SSL-VPN çözümü sağlamalı. Önerilen çözüm kullanıcı/grup tabanlı SSL-VPN erişimi sağlamalıdır (Sınırsız kullanıcı için ücretsiz lisans olmalıdır)
10,15 Önerilen çözüm, Uzak Ethernet Cihazları vasıtası ile uzak ağın IP yönetimi, DHCP ve DNS yönetimini yapabilmelidir.
10,16 Önerilen çözüm, Uzak Ethernet Cihazları vasıtası ile farklı lokasyonlar arası VPN bağlantısı yapabilmelidir.
10,17 Önerilen çözüm, RDP, HTTP, HTTPS, SSH, Telnet ve VNC desteği için benzersiz şifreli HTML5 self servis portalına sahip olmalıdır.

Kayıt ve Raporlama

11,01 Önerilen çözüm internet gizlilik yasalarına uyması için Data Anonymization özeliğini desteklemelidir
11,02 Önerilen çözüm cihaz üzerinde dahili raporlamaya sahip olmalıdır.
11,03 Önerilen çözüm en as 1000+ raporlama seçeneği sunmalıdır.
11,04 Önerilen çözüm raporları Excel ve PDF biçimlerinde dışarı verebilmelidir.
11,05 Önerilen çözüm Antivirüs, içerik filtreleme, trafik tanımlama, IPS ve Firewall'un syslog sunucusu üzerinde kütüklerinin tutulmasını desteklemelidir.
11,06 Önerilen çözüm HTTP ya da HTTPS protokolü üzerinde gönderilen tüm dosyalar hakkında ayrıntılı raporlama yapmalıdır. Rapor kullanıcı adı, IP adresi, bağlantı, dosya adı,

tarih ve saati içermelidir. Önerilen çözüm uygulama, kullanıcı ve IP adresi bazlı veri transfer raporu sunabilm
11,07 Önerilen çözüm kullanıcı, kaynak IP, hedef IP, kaynak port, hedef port ya da protokol tabanlı veri transfer raporları hazırlayabilmelidir.
11,08 Önerilen çözüm kullanıcı, kaynak IP, hedef IP, kaynak port, hedef port ya da protokol tabanlı bağlantı raporları hazırlayabilmelidir.
11,09 Önerilen çözüm raporları e-posta adreslerine gönderebilmelidir.
11,10 Önerilen çözümü SOX, HIPPA, PCI, FISMA ve GLBA uyumlu rapor yaratabilmelidir.
11,11 Önerilen çözüm cihazın tüm faaliyetini denetleme olanağı sunmalıdır.
11,12 Önerilen çözüm uzak kayıt için çoklu syslog sunucularını desteklemelidir.
11,13 Önerilen çözüm tüm modüllerin kayıt bilgilerini syslog sunucularına göndermelidir.
11,14 Önerilen çözüm raporların belirtilen bir e-posta adresine gönderecek şekilde ayarlanabilmelidir.
11,15 Önerilen çözüm firewall'dan geçen tüm mesajlar hakkında detaylı rapor sunmalıdır.
11,16 Önerilen çözüm kullanıcı/IP adresi tarafından yapılan tüm engellenen girişimleri raporlamalıdır.
11,17 Önerilen çözüm UTM, proxy (vekil) Firewall'lar, Özel uygulamalar ve Syslog uyumlu cihazların kayıt ve raporlarının türetilebilmesini sağlamalıdır.
11,18 Önerilen çözüm özelleştirilebilmesi için değiştirilebilir çoklu kontrol paneli raporlamasını desteklemelidir.
11,19 Önerilen çözüm güvenlik sızıntısının gerçekleştiği andaki olayları tekrarlayabilmeleri için organizasyonlara yardımcı olması amacıyla araştırma imkanı sunmalıdır.

Uygulama Filtreleme Çözümü

12,01 Önerilen çözüm dahili Uygulama Filtreleme çözümü sağlamalıdır.
12,02 Önerilen çözüm uygulamaları port, protokol ve SSL/TLS şifrelemesi ile tanımlayabilmelidir (izin verme/engelleme/kaydetme)
12,03 Önerilen çözüm 3000+ uygulamayı kontrol edebilmelidir.
12,04 Önerilen çözümün uygulama veri tabanı manüel müdahaleye gerek olmadan otomatik güncellenmelidir
12,05 Önerilen çözüm kimlik bazlı raporlan oluşturabilmelidir (IP yanında kullanıcı adı)
12,06 Önerilen çözüm aşağıdaki uygulamaları engelleyebilmelidir:

a. Dosya aktarımına izin veren uygulamalar
b. Çevrimiçi oyunlar
c. Anında Mesajlaşma Yazılımları (İngilizce olmayanlar dahil)
c. Peer-to-Peer (P2P) uygulamaları (İngilizce olmayanlar dahil)
e. Gezgin tabanlı proxy (vekil) sunucu (IP adresi ya da porttan bağımsız)
f. Web 2.0 tabanlı uygulamalar (Facebook, CRM vs.)
g. Uzaktan Kontrol sağlayan uygulamalar
h. Tüm canlı medya tipleri (Web ve yazılım tabanlı)
i. VOIP Uygulamaları

12,07 Önerilen çözüm standart portlar üzerinde çalışan gizli uygulamaları tanımlayabilmelidir (80, 443, 22 vs.)

Lisanslama ve Garanti Süresi

13,1 Önerilen çözüm 1 yıl boyunca antivirüs, içerik ve uygulama filtreleme, saldırı tespit ve engelleme, lisanslarının güncellemelerini alabilmelidir.
13,2 Önerilen çözümün donanım garantisi en az 1 yıl olmalıdır.