# **ssİNTERNET İYİLEŞTİRME İHALESİ TEKNİK ŞARTNAME**

# Omurga Anahtar (2 Adet)

1. Teklif edilecek omurga anahtarın üreticisi, 2021 Enterprise Wired and Wireless LAN Infrastructure tarafında Gartner Magic Quadrant raporlarında Liderler ve Vizyonerler kategorisinde yer almalıdır.
2. Anahtar üzerinde en az 48 adet 1/10G SFP+ port ve 6 adet 40G QSFP+ port bulunacaktır.
3. Her bir cihaz ile birlikte 1 adet 3 metrelik 40G DAC kablo teklife dahil edilecektir.
4. Cihazın anahtarlama kapasitesi en az 2.5 Tbps ve paket iletim performansı en az 1900 Mpps olmalıdır.
5. Teklif edilecek anahtar en az 4GB RAM ve 8GB flash memory’e sahip olmalıdır.
6. Anahtar yığınlanabilir yapıda olmalıdır. VSF, IRF, VSU, VSX vb. özellikleri desteklemelidir.
7. Anahtarın güç üniteleri yedeklenebilir olmalıdır ve yedekli şekilde teklif edilecektir.
8. Anahtarın syslog desteği olmalıdır.
9. Anahtar LLDP özelliğini desteklemelidir.
10. Anahtar SNMP v1/v2c/v3 desteğine sahip olmalıdır.
11. Anahtarlama cihazı, ağ üzerindeki döngüleri engelleyecek, ağın kararlılığını artırmak ve fiziksel yedeklilik sağlamak amacı ile IEEE 802.1d Spanning Tree, IEEE 802.1w Rapid Spanning Tree ve IEEE 802.1s Multiple Spanning Tree protokollerini destekleyecektir.
12. Anahtar LACP desteğine sahip olmalıdır.
13. Anahtar Layer 3 düzeyinde VRRP, VRRPE vb. protokolleri desteklemelidir.
14. Anahtar DHCP Server özelliğine sahip olmalıdır.
15. Anahtar 802.1Q VLAN standartlarını desteklemelidir. 4000 adet VLAN ID desteklemelidir.
16. Teklif edilecek anahtar Static Routing, OSPF, BGP ve Policy Based Routing özelliklerini destekleyecektir. Bu özellikler bir lisans gerektiriyorsa teklife dahil edilecektir.
17. Hat yedekliliği ve bant genişliği kontrolü yapan ECMP(Equal-cost multipath) ile yük paylaşımı(load-balancing) yapabilmelidir.
18. Anahtar üzerinde, IP kaynak/hedef adreslerine göre UDP/TCP port numarasına göre ACL yazılabilmelidir.
19. Anahtarlama cihazının QoS desteği bulunacaktır. Cihaz, IEEE 802.1p Priority Queuing desteğine sahip olmalıdır.
20. Teklif edilen anahtar geleneksel mimaride kullanılabildiği gibi, kendi üreticisine ait bulut platform üzerinden de yönetilebilmeli ve monitor edilebilmelidir.

# Tip 1 Kenar Anahtar (1 Adet)

1. Teklif edilecek omurga anahtarın üreticisi, 2021 Enterprise Wired and Wireless LAN Infrastructure tarafında Gartner Magic Quadrant raporlarında Liderler ve Vizyonerler kategorisinde yer almalıdır.
2. Anahtar üzerinde en az 48 adet 10/100/1000 Base-T PoE+ port ve 4 adet 10Gbit SFP+ bulunmalıdır.
3. Anahtarın üzerinde USB portu ve OutofBand Management portu olmalıdır.
4. Anahtar istendiğinde yığınlanabilir (Stackable) yapıda olmalı ve enaz 8 adet anahtar ring veya chain yöntemiyle yığınlanabilmelidir. Yığınlama bantgenişliği en az 40Gbps olmalıdır.
5. 10/100/1000 portlar Auto-MDIX özelliğine sahip olmalı böylelikle çapraz veya düz bağlantı ayarlaması otomatik olarak yapılmalıdır.
6. IEEE 802.3af PoE ve IEEE 802.3at PoE+ özellikleri anahtar bazında tüm UTP portlarda standart olarak bulunmalıdır. Anahtar 370 Watt PoE bütçesi sağlamalıdır.
7. Cihazin backplane kapasitesi en az 176 Gbps, data iletim kapasitesi en az 112 million pps olmalıdır.
8. Latency (gecikme) degeri gigabit ve 10 gigabit portlar için 4 mikrosaniyeden fazla olmamalıdır.
9. Adres tablosunda en az 32000 adet MAC adresi destegi olmalıdır.
10. Cihaz en az single area OSPF v2 ve OSPF v3 desteklemelidir ve bu özellikle öenrilmelidir. OSPF desteği Stub Area ve NSSA ile sınırlı olmamalıdır.
11. Yönlendirme tablosunda en az 10.000 adet yön bilgisi tutulabilmelidir.
12. Ürün Policy Based routing desteklemeli ve bu özellik kullnılabilir şekilde gerekli lisanslarla önerilmelidir.
13. Anahtarın toplam en az 12MB packet buffer kapasitesi olmalıdır.
14. Birden fazla konfigürasyon dosyası tutulması için yeterli Flash bellek ile teklif edilmelidir.
15. Cihazın işletim sisteminin güncellenmesi esnasında yedeklilik için birbirinden bağımsız iki imaj desteği olmalıdır.
16. IEEE 802.3ad link aggregation özelliği ile 8 portu destekleyen bağlantı noktası (Trunk) oluşturulabilmelidir. IEEE 802.3ad link aggregation özelliği ile yığında 60 adet bağlantı noktası (Trunk) oluşturulabilmelidir.
17. IEEE 802.1Q (4,094 VLAN ID) VLAN ID’si işaretleme desteği ve en az 256 adet port bazında VLAN tanımlanabilmelidir. GVRP veya benzeri bir protokol ile otomatik olarak VLAN’ları öğrenebilmeli ve atama yapabilmelidir. IEEE 802.1v protokolü desteği ile VLAN seçimi Layer 3 protokole göre yapılabilmelidir.
18. IEEE 802.1D STP, IEEE 802.1s MSTP, IEEE 802.1w RSTP protokollerini desteklemelidir.
19. En az 9200 byte büyüklüğünde yüksek boyutlu iletim birimi (Jumbo Frame) desteği bulunmalıdır.
20. Layer 3 yönlendirme desteklenecektir. Statik yönlendirme, RIPv1 ve RIPv2 desteği olacaktır.
21. Hat yedekliliği için ECMP desteği olacaktır.
22. Gereksiz yayın trafiğinin engellenmesi için IGMPv1,v2,v3 desteği olmalıdır.
23. Yeni jenerasyon IPv6 desteği bulunmalıdır. IPv4 protokolünden IPv6 protokolüne geçiş için her iki protokolün kullanımına imkan vermelidir. IPv6 host desteği bulunmalıdır.
24. IP kaynak/hedef adreslerine göre, UDP/TCP port numarasına göre Access Control List’ler (ACL) yazılabilmelidir.
25. Port güvenliği özelliği ile kullanıcı listeleri oluşturularak sadece belli MAC adreslerinin ilgili portlara bağlantı kurmasına izin verilebilmelidir. Bu sayede izinsiz kullanıcı ve cihazların ağa girişleri engellenebilmelidir.
26. RADIUS ve TACACS+ protokolleri ile kimlik tanımlama özelliklerini desteklemelidir. Anahtarı yönetmek isteyen kişiler Radius sorgulama protokolü tarafından sorgulanabilmelidirler.
27. IEEE 802.1x kimlik tanımlama protolü desteği bulunmalıdır. Port bazında Web tabanlı ve MAC adresi tabanlı kimlik tanımlama metodunu desteklemelidir.
28. Port başına aynı anda birden fazla kimlik tanımlama metoduna (802.1x, Web Tabanlı, Mac Tabanlı) ve port başına aynı anda birden fazla 802.1x kullanıcısı desteği bulunmalıdır.
29. Kimlik kontrolüne bağlı VLAN ataması gerçekleştirilebilmelidir.
30. Kimlik kontrolüne bağlı erişim kontrolü (ACL) yapılabilmelidir.
31. İstenmeyen ARP Broadcast saldırılarına karşın güvenlik önlemi olarak dinamik ARP koruması özelliği bulunmalıdır.
32. Port başına gereksiz yayın (broadcast) trafiğini engelleme mekanizması olmalıdır.
33. Hangi anahtarlama portlarının birbirleriyle görüşeceğini kontrol etmek için kaynak port filtrelemesi veya benzeri özelliği bulunmalıdır.
34. İstenmeyen DHCP sunucularına karşın güvenlik önlemi olarak DHCP koruması özelliği bulunmalıdır.
35. BPDU ataklarına karşın STP BPDU port koruması bulunmalıdır. STP Root olarak seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı koruma özelliği bulunmalıdır.
36. SSHv2 Secure Shell protokolü ile uzaktan güvenli şekilde yönetilebilir olmalıdır.
37. İstek dışı multicast baskınlarına karşı IP multicast snooping desteği bulunmalıdır.
38. SNMPv1,v2,v3 ve RMON protokolleri desteklenmelidir. Herhangi bir tarayıcı ile HTML tabanlı, HTTP ve HTTPS protokolleri ile uzaktan yönetilebilir olmalıdır. Secure Sockets Layer (SSL) protokolü desteklenmelidir.
39. sFlow veya NetFlow gibi veri akışı izleme protokollerinin en az birinin desteği bulunmalıdır.
40. Network trafiğini takip etmek için Port-Monitoring özelliği bulunmalıdır.
41. Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı Uni-Directional Link Detection (UDLD) desteği bulunmalıdır.
42. IEEE 802.1AB Link Layer Discovery Protocol (LLDP) keşif protokolü veya benzeri bir protokol desteği bulunmalıdır. Destekli IP Telefon gibi uç cihazların QoS ve Vlan gibi ayarlarının otomatik olarak yapılabilmesi için LLDP-MED protokolü desteği bulunmalıdır.
43. Hız sınırlama (Rate Limiting) özelliği olmalıdır.

# Tip 2 Kenar Anahtar (8 Adet)

1. Teklif edilecek omurga anahtarın üreticisi, 2021 Enterprise Wired and Wireless LAN Infrastructure tarafında Gartner Magic Quadrant raporlarında Liderler ve Vizyonerler kategorisinde yer almalıdır.
2. Anahtar üzerinde en az 24 adet 10/100/1000 Base-T PoE+ port ve 4 adet 10Gbit SFP+ bulunmalıdır.
3. Anahtarın üzerinde USB portu ve OutofBand Management portu olmalıdır.
4. Anahtar istendiğinde yığınlanabilir (Stackable) yapıda olmalı ve enaz 8 adet anahtar ring veya chain yöntemiyle yığınlanabilmelidir. Yığınlama bantgenişliği en az 40Gbps olmalıdır.
5. 10/100/1000 portlar Auto-MDIX özelliğine sahip olmalı böylelikle çapraz veya düz bağlantı ayarlaması otomatik olarak yapılmalıdır.
6. IEEE 802.3af PoE ve IEEE 802.3at PoE+ özellikleri anahtar bazında tüm UTP portlarda standart olarak bulunmalıdır. Anahtar 370 Watt PoE bütçesi sağlamalıdır.
7. Cihazin backplane kapasitesi en az 128 Gbps, data iletim kapasitesi en az 95 million pps olmalıdır.
8. Latency (gecikme) degeri gigabit ve 10 gigabit portlar için 4 mikrosaniyeden fazla olmamalıdır.
9. Adres tablosunda en az 32000 adet MAC adresi destegi olmalıdır.
10. Cihaz en az single area OSPF v2 ve OSPF v3 desteklemelidir ve bu özellikle öenrilmelidir. OSPF desteği Stub Area ve NSSA ile sınırlı olmamalıdır.
11. Yönlendirme tablosunda en az 10.000 adet yön bilgisi tutulabilmelidir.
12. Ürün Policy Based routing desteklemeli ve bu özellik kullnılabilir şekilde gerekli lisanslarla önerilmelidir.
13. Anahtarın toplam en az 12MB packet buffer kapasitesi olmalıdır.
14. Birden fazla konfigürasyon dosyası tutulması için yeterli Flash bellek ile teklif edilmelidir.
15. Cihazın işletim sisteminin güncellenmesi esnasında yedeklilik için birbirinden bağımsız iki imaj desteği olmalıdır.
16. IEEE 802.3ad link aggregation özelliği ile 8 portu destekleyen bağlantı noktası (Trunk) oluşturulabilmelidir. IEEE 802.3ad link aggregation özelliği ile yığında 60 adet bağlantı noktası (Trunk) oluşturulabilmelidir.
17. IEEE 802.1Q (4,094 VLAN ID) VLAN ID’si işaretleme desteği ve en az 256 adet port bazında VLAN tanımlanabilmelidir. GVRP veya benzeri bir protokol ile otomatik olarak VLAN’ları öğrenebilmeli ve atama yapabilmelidir. IEEE 802.1v protokolü desteği ile VLAN seçimi Layer 3 protokole göre yapılabilmelidir.
18. IEEE 802.1D STP, IEEE 802.1s MSTP, IEEE 802.1w RSTP protokollerini desteklemelidir.
19. En az 9200 byte büyüklüğünde yüksek boyutlu iletim birimi (Jumbo Frame) desteği bulunmalıdır.
20. Layer 3 yönlendirme desteklenecektir. Statik yönlendirme, RIPv1 ve RIPv2 desteği olacaktır.
21. Hat yedekliliği için ECMP desteği olacaktır.
22. Gereksiz yayın trafiğinin engellenmesi için IGMPv1,v2,v3 desteği olmalıdır.
23. Yeni jenerasyon IPv6 desteği bulunmalıdır. IPv4 protokolünden IPv6 protokolüne geçiş için her iki protokolün kullanımına imkan vermelidir. IPv6 host desteği bulunmalıdır.
24. IP kaynak/hedef adreslerine göre, UDP/TCP port numarasına göre Access Control List’ler (ACL) yazılabilmelidir.
25. Port güvenliği özelliği ile kullanıcı listeleri oluşturularak sadece belli MAC adreslerinin ilgili portlara bağlantı kurmasına izin verilebilmelidir. Bu sayede izinsiz kullanıcı ve cihazların ağa girişleri engellenebilmelidir.
26. RADIUS ve TACACS+ protokolleri ile kimlik tanımlama özelliklerini desteklemelidir. Anahtarı yönetmek isteyen kişiler Radius sorgulama protokolü tarafından sorgulanabilmelidirler.
27. IEEE 802.1x kimlik tanımlama protolü desteği bulunmalıdır. Port bazında Web tabanlı ve MAC adresi tabanlı kimlik tanımlama metodunu desteklemelidir.
28. Port başına aynı anda birden fazla kimlik tanımlama metoduna (802.1x, Web Tabanlı, Mac Tabanlı) ve port başına aynı anda birden fazla 802.1x kullanıcısı desteği bulunmalıdır.
29. Kimlik kontrolüne bağlı VLAN ataması gerçekleştirilebilmelidir.
30. Kimlik kontrolüne bağlı erişim kontrolü (ACL) yapılabilmelidir.
31. İstenmeyen ARP Broadcast saldırılarına karşın güvenlik önlemi olarak dinamik ARP koruması özelliği bulunmalıdır.
32. Port başına gereksiz yayın (broadcast) trafiğini engelleme mekanizması olmalıdır.
33. Hangi anahtarlama portlarının birbirleriyle görüşeceğini kontrol etmek için kaynak port filtrelemesi veya benzeri özelliği bulunmalıdır.
34. İstenmeyen DHCP sunucularına karşın güvenlik önlemi olarak DHCP koruması özelliği bulunmalıdır.
35. BPDU ataklarına karşın STP BPDU port koruması bulunmalıdır. STP Root olarak seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı koruma özelliği bulunmalıdır.
36. SSHv2 Secure Shell protokolü ile uzaktan güvenli şekilde yönetilebilir olmalıdır.
37. İstek dışı multicast baskınlarına karşı IP multicast snooping desteği bulunmalıdır.
38. SNMPv1,v2,v3 ve RMON protokolleri desteklenmelidir. Herhangi bir tarayıcı ile HTML tabanlı, HTTP ve HTTPS protokolleri ile uzaktan yönetilebilir olmalıdır. Secure Sockets Layer (SSL) protokolü desteklenmelidir.
39. sFlow veya NetFlow gibi veri akışı izleme protokollerinin en az birinin desteği bulunmalıdır.
40. Network trafiğini takip etmek için Port-Monitoring özelliği bulunmalıdır.
41. Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı Uni-Directional Link Detection (UDLD) desteği bulunmalıdır.
42. IEEE 802.1AB Link Layer Discovery Protocol (LLDP) keşif protokolü veya benzeri bir protokol desteği bulunmalıdır. Destekli IP Telefon gibi uç cihazların QoS ve Vlan gibi ayarlarının otomatik olarak yapılabilmesi için LLDP-MED protokolü desteği bulunmalıdır.
43. Hız sınırlama (Rate Limiting) özelliği olmalıdır.

# Transceiver

1. Cihazlar ile birlikte aynı üreticiye ait toplam 42 adet 10G-SR transceiver, 54 adet 1G-SX transceiver teklife dahil edilecektir.
2. Önerilen ürünler kesinlikle OEM olarak teklif edilmeyecektir.

# Access Point (75 Adet)

1. Teklif edilecek Access Point’in üreticisi, 2021 Enterprise Wired and Wireless LAN Infrastructure tarafında Gartner Magic Quadrant raporlarında Liderler ve Vizyonerler kategorisinde yer almalıdır.
2. Cihaz çift radyolu olmalı ve ETSI standartlarında 2.4 GHz ve 5 GHz frekans bandında çalışabilmelidir. Cihaz akıllı bir algoritma sayesinde, içinde bulunduğu RF ortamına göre farklı modlarda çalışabilmelidir.
3. Cihaz üzerinde 2.4 Ghz bandında en az 4 dBi, 5 Ghz bandında en az 7 dBi pik anten kazancına sahip dahili antenler bulunmalıdır.
4. Cihaz 802.11n, 802.11ac ve 802.11ax standartlarını desteklemelidir.
5. Cihazın 802.11ax 4x4 MIMO desteği bulunmalıdır
6. Cihaz 802.11ax teknolojisinde 2.4Ghz radio için 574mbps ve 5Ghz radio için 4.8Gbps hızları desteklemelidir.
7. Cihaz OFDMA (Orthogonal Frequency Division Multiple Access) desteğini sunmalıdır.
8. Cihaz 1024 QAM modülasyon tipini desteklemelidir.
9. Cihaz 20/40/80/160 Mhz kanallarını desteklemelidir.
10. Teklif edilen kablosuz erişim cihazı Advanced Cellular Coexistence (ACC) ve Dynamic Frequency Selection(DFS) özelliklerine sahip olacaktır.
11. Cihaz üzerinde 1 adet 100/1000 Base-T port ve 1 adet 100/1000/2500 Base-T port bulunmalıdır.
12. Cihazın LACP desteği bulunmalıdır.
13. Cihaz üzerinde dahili Bluetooth ve Zigbee radyoları bulunmalıdır.
14. Cihaz WPA,WPA2 ve WPA3 desteğine sahip olmalıdır.
15. Önerilecek cihaz herhangi bir controller gerektirmeyen instant mimariyi, controller-tabanlı mimariyi ve bulut-tabanlı mimariyi destekleyecektir. Desteklenmeyen durum açıkça belirtilecektir.
16. Cihaz spectrum analyzer yeteneğine sahip olmalıdır. Bu özelliği sayesinde enterferansa karşı kendini iyileştirme ve optimizasyon yapabilmelidir.
17. Cihaz ortam taraması yaparak kablosuz saldırı engelleme sistemlerinin sensoru şeklinde çalışabilmelidir. Kapsama alanı içinde bulunan kuruma ait olmayan kablosuz erişim noktalarını da tespit edebilmelidir.
18. Cihaz, merkezi yönetim donanımı/yazılımı ile birlikte çalışarak Layer 7 uygulama kontörlü için DPI (deep paket inspection) desteklemelidir.

# Wireless Controller (1 Adet)

1. Teklif edilecek Access Point’in üreticisi, 2021 Enterprise Wired and Wireless LAN Infrastructure tarafında Gartner Magic Quadrant raporlarında Liderler ve Vizyonerler kategorisinde yer almalıdır.
2. İstenilen merkezi yönetim donanımı en az 256 adet AP’ye aynı anda hizmet verebilecek slot sayısına, veriyoluna ve güç kaynağına sahip olmalıdır. Bu şartnamede istenen tüm özellikler 1Uluk tek bir donanımla sağlanmalıdır.
3. Cihaz ile birlikte 75 adet AP için gerekli lisanslar teklife dahil edilecektir.
4. Kablosuz ağ kontrol cihazı ve bağlı olduğu donanım/yazılımlar ile, tüm AP’lerin kanal, çıkış gücü vs. ayarlamalarını otomatik yapmalı, değişen koşullara, enterferans/gürültü durumlarına, ortamdaki yabancı kablosuz ağ donanımlarına göre çıkış gücü ve kanalları otomatik değiştirebilmelidir. Ortamda mikrodalga, bluetooth vb. enterferans kaynakları varsa, kablosuz ağ kontrol kartı bunu tespit ederek, AP’leri farklı kanallara otomatik atayabilmelidir. Aynı kapsama alanında bir AP’nin servis vermemesi, diğer AP’ler tarafından fark edilebilmeli, komşu AP’ler otomatik olarak yayın güçlerini artırıp servis vermeyen AP’den kaynaklı RF kapsama boşluğunu azaltmaya çalışmalıdır.
5. Kablosuz ağ kontrol cihazı ve bağlı olduğu donanım/yazılımlar ile, aynı kapsama alanına hizmet veren iki AP arasında kullanıcılara yük paylaşımı yapabilmelidir. Bu yük paylaşımı, kullanıcı sayısına göre ayarlanabilmelidir. Kullanıcı tarafındaki sinyal gücü daha düşük bile olsa, belli kullanıcıların, belli AP’lere bağlanabilmesini sağlayabilmelidir. İlgili donanım, RF spektrumunu kullanıcılar arası adil paylaştırmaya yönelik teknolojilere sahip olmalıdır.
6. Sistem kullanıcı bağlı ve sistemde trafik yaratırken dahi kullanıcıyı bağlı olduğu erişim noktasından başka bir erişim noktasına taşıyabilmeli, bu sayede yük dengelemesini sürekli yapabilmelidir. Aynı zamanda erişim noktaları arasında dolaşım yapması gerekirken yapmayan kullanıcıları da bağlı olmaları gereken erişim noktalarına taşıyabilmeli bu sayede yapışkan kullanıcı problemini de çözebilmelidir.
7. Kablosuz ağ merkezi yönetim donanımı, tüm kablosuz ağ trafiğini kendi üzerinden geçirecek şekilde tasarlanmış olmalıdır. Sistem, tüm trafiğin merkezi yönetim donanımı üzerinden geçeceği şekilde çalıştırılacaktır.
8. Kablosuz ağ merkezi yönetim donanımı 256 yerel ağa yada uzak ağa bağlı AP destekleyebilmeli ve cihazın 12 Gbps firewall performansi olmalıdır.
9. Kablosuz ağ merkezi yönetim donanımı, istendiğinde ilave lisans ile yönettiği tüm AP’lerin kapsama alanlarında elle veya otomatik olarak rouge AP / enterferans oluşturan AP tespiti yapmalı, AP’leri yetkilendirilmiş, izinsiz (rogue), sınıflandırılmamış, yanlış ayarlanmış vb. şeklinde sınıflara ayırmalı, “de-authentication” paketleri göndererek rouge AP’lerin servis vermesini önlemelidir (Rouge AP containment).
10. Kablosuz ağ merkezi yönetim donanımı, birden fazla bandda farklı MAC adresleriyle yayın yapan bir AP'yi tek bir AP seklinde gösterebilmelidir.
11. Kurulacak sistemde, bir kullanıcının bir AP’nin kapsama alanından diğer bir AP’nin kapsama alanına geçerken hissetmeyeceği şekilde bağlantı verecek “mobility” özelliği bulunmalıdır. Bu “mobility” özelliği kullanıcı güvenli/şifreli yetkilendirme mekanizması ile ağa bağlıyken, merkezi yönetim cihazları aynı alt ağ maskesi taşıyan ağ içinde (L2 mobility) veya başka VLAN’lara ait ağlara hizmet veriyorken (L3 mobility) de sağlanacaktır. L3 mobility sırasında kullanıcının IP adresi değişmeyecektir.
12. Kablosuz ağ merkezi yönetim donanımı tek başına yerleşke yerel ağına bağlı veya uzak aga bagli en az 256 AP’ye aynı anda destek verebilecek kapasitede olmalıdır.
13. Kablosuz ağ merkezi yönetim donanımı ile, misafir kullanıcılara bir web arayüzü çıkartarak buradan yetkilendirme yapılması mümkün olmalıdır. Firmanın önereceği markaya ait donanım/yazılımlarda, misafir kullanıcılara değişik haklar ve sınırlamalar tanımlanabileceği bir çözüm sunulabilmelidir. (belli bir VLAN’a atama, belli bir süre sistemi kullanma, belli IP bloklarına erişim vs.). Kullanıcıya çıkacak web arayüzü İdare tarafından özelleştirilebilmeli, gerektiğinde harici bir başka web sunucuya yönlendirilebilmelidir. Kullanıcılara çıkartılacak web arayüzünden girilecek şifre bilgileri, İdarenin kullandığı Radius /Ldap sunucuları üzerinden yetkilendirilebilmelidir.
14. Sistemde o anda toplam kaç kullanıcının olduğu, hangi AP’ye kaç kullanıcının bağlandığı, AP’lerin oluşturduğu trafikler vb. şekilde bilgiler elde edilebilmelidir. Bu bilgiler, ya merkezi donanımlar üzerindeki raporlama araçları kullanılarak elde edilebilmeli ya da SNMP ile periyodik sorgulamaların harici bir ortamda grafiklenmesi şeklinde olmalıdır.
15. Tüm AP’lerin yazılım versiyonu merkezi olarak denetlenebilmeli, yeni bir yazılım, merkezi donanıma eklendiği an, otomatik olarak tüm ağ cihazlarına aynı anda yazılım yükseltmesi yapılabilmelidir.
16. Merkezi yönetim donanımı ssh (v2), https protokolleri kullanılarak yönetilebilmelidir.
17. Firmanın önereceği markaya ait donanım/yazılımlarda, IP multicast (Layer2 ve Layer3) desteği ve kullanıcılara belli bir maksimum band genişliğinde data çekimi tahsis edilebileceği bir QoS (Quality of Service) çözümü olmalıdır.
18. Merkezi yönetim donanımı , ipv6 protokolünden anlayabilmeli, ipv6 adresine sahip kullanıcılara hizmet verebilmeli, üzerinde ipv6 servisleri tanımlanabilir olmalıdır. Kontrol birimi üzerinde ipv6 adresine sahip kullanıcılar görülebilmelidir.
19. DHCP sunucu servisi verme, DHCP isteklerini yönlendirme (DHCP relay) yapabilmeli, DHCP option 82 özelliğini kullanabilmelidir.
20. Merkezi yönetim donanımı OSPF yönlendirme protokolünü desteklemelidir. Cihaz, bir bölge için OSPF işlemi çalıştırarak farklı IP Blokları arası paket yönlendirmesi yapabilmelidir.
21. Kurulacak kablosuz ağ sisteminin donanımsal ve yazılımsal tasarımının WPA2-Enterprise (802.1X kullanımı için) uyumlu olmalıdır. Tüm EAP (EAP-TTLS gibi) tiplerinin sorunsuz olarak çalışmasını desteklemelidir.
22. Merkezi yönetim işlerinde kullanılan tüm donanımların üzerinde takılı olan flash disk ve RAM’ler, donanımsal olarak desteklenen en üst kapasitede ve hızda olacaktır.
23. Kablosuz ağ merkezi yönetim donanımı, kendisine bağlı AP'lerin, ortamdaki en uygun kanalı belirlemek için yaptığı RF taramalar sırasında, ortamda yüksek yoğunlukta trafik oluşturan kullanıcılar varsa, RF tarama özelliğini erteleyebilmelidir.
24. Kablosuz ağ merkezi yönetim donanımı, belli bir SSID’ye baglanilmasini, belirli zaman araliklarinda engelleyebilmelidir.
25. Tüm kablosuz ağ trafiği, merkezi donanım üzerinden geçmeli ve bu donanım, tüm trafiği statefull özelliğine sahip bir firewall mekanizması üzerinden geçirebilmelidir. Bu özellik ilave bir lisans veya donanım gerektiriyorsa teklife dahil edilmeli ve istenen yapı kurulmalıdır.
26. Firewall özelliği sayesinde, herhangi bir bantgenişliği kısıtlaması olmaksızın, merkezi donanım cihazı üzerinden geçen tüm trafik, herhangi bir darboğaz oluşturmadan ve yavaşlamaya maruz kalmadan, aynı hız ile firewall denetiminden de geçirilebilmelidir.
27. Tüm trafiğin tüm firewall yeteneklerinden faydalanılarak denetlenmesi durumunda sistemin genel bantgenişliği kapasitesinde herhangi bir düşüş yaşanmamalıdır.
28. Sisteme dahil olacak kullanıcıların erişimleri firewall denetimlerinden geçmeli ve istenildiğinde sadece belirli IP bloklarına istenilen servislerle erişimleri sağlanmalıdır.
29. Sistemdeki firewall rol bazlı olup, kablosuz ağa bağlanan her bir kullanıcı için ayrı ayrı roller tanımlanabilmelidir. Bu sayede, roller arasi trafik yukarıdaki belirtilen performans kriterlerine uymak suretiyle denetlenebilmelidir. Bu özellik ilave bir lisans veya donanım gerektiriyorsa teklife dahil edilmeli ve istenen yapı kurulmalıdır.
30. Cihaz uygulamaları tanırken DPI yönetenini kullanacaktır.
31. Cihaz ağ içeriğini sınıflandırabilmelidir.
32. Cihaz tek başına çalışırken aynı anda 8000 kullanıcıya hizmet verebilmelidir..
33. Cihaz RF taramaları esnasında ortamda ses, video trafiği var ise bu taramaları erteleyebilmelidir.
34. Cihaz, kullanıcılar bağlıyken, kullanıcıların Yük dengelemesini yapabilmeli, Kullanıcılar bağlıyken 5 GHz desteği olan Kullanıcıları 5 GHz bandına taşıyabilmelidir.
35. Kablosuz köprü bağlantılarının, SSID masquerade ataklarının, tanımlanamayan MAC OUI’lerin ve çalınmış kullanıcı MAC adreslerinin tespiti yapılmalıdır.
36. Cihaz istendiğinde ilave lisans arttırımı ile rogue AP’lerin “man in the middle” saldırı yapmasını önleyebilme ve bu AP’lerde “beacon rate” analizi yapabilme, yanlış yapılandırılmış AP’leri önleme özelliğinin olması gerekmektedir.
37. BSSID'ye, hedef MAC adresine, kaynak MAC adresine 802.11 paketlerinin sıra numarası kısmına bağlı olarak yeni imzalar ekleyebilme, her bir kanalda çerçeve oranı (frame rate) analiz yönetimi ve kontrolü yapılabilmelidir.
38. Networke giriş kurallarını önceden belirlenecek sürelerde otomatik olarak devreye alabilme veya devreden çıkarabilme. Bu sayede, mesai saatlerinde belli servislerin (FTP, VPN, Web vb.) otomatik olarak devreye alınabilmeli veya devreden çıkarılabilmelidir.
39. Cihaz istendiğinde ilave lisans arttırımı ile belirli bir alan dahilinde, sistemden kablosuz olarak hizmet alan kullanıcıların, sadece sisteme ait SSID’lere bağlanmasına izin verebilmeli, kullanıcı bilgisayarlarına herhangi bir client yazılımı yüklenmesine gerek olmaksızın, kullanıcıların ortamda bulunan ve sisteme ait olmayan diğer SSID’lere bağlanmalarını engelleyebilmelidir.
40. 802.11 ortamına yapılan atakları tespit edebilme özelliğine sahip olmalıdır.
41. Cihaz üzerinde en az 4 adet Gigabit (1000Base-X) SFP veya 10/100/1000BASE-T çalışabilen port ve 2 adet 10 Gb (10Gbase-X) SFP+ modül yuvası olmalıdır.
42. Sistem minimum es zamanli 1 milyon firewall oturumunu desteklemelidir. Desteklemiyorsa eş değer kapasitede firewall konumlandırılmalı, istenen yapı, gerekli ek lisans ve donanım ile sağlanacak şekilde teklife dahil edilmelidir.
43. Cihaz ile birlikte en az 3 yıllık NBD support paketi teklife dahil edilmelidir.