1. GELİŞMİŞ SALDIRI E-POSTA ANALİZ VE ENGELLEME SİSTEMİ TEKNİK ŞARTNAMESİ

1.1. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemini oluşturan tüm bileşenler aynı üreticiye ait tek bir ürün olacaktır. Aynı üreticiye dahi ait olsa farklı ürünlerin bir araya getirilmesinden oluşturulan bir çözüm olmayacaktır.

1.2. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, e-posta tabanlı saldırıları tespit edebilen ve engelleyebilen tek bir amaca yönelik cihaz (appliance) biçiminde olacaktır.

1.3. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi üzerinde en az 4 (dört) adet 1 (bir) Gbps ethernet ara yüzü bulunacaktır.

1.4. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi üzerinde en az 2 (iki) adet her biri en az 6 (altı) çekirdekli işlemci ve en az 64 (altmış dört) GB bellek bulunacaktır.

1.5. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi üzerinde donanımsal RAID desteğine sahip en az 2 (iki) adet 600 (altıyüz) Gb kapasiteli sabit disk bulunacaktır.

1.6. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üzerinde yedekli güç kaynakları bulunacaktır.

1.7. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, aynı ve farklı üreticilere ait SMTP Ağ Geçidi çözümleri ile tam uyumlu çalışacaktır.

1.8. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, MTA, SPAN/TAP ya da BCC çalışma şekillerini destekleyecektir.

1.9. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, MTA olarak çalıştığında, zararlı olarak tespit edilen epostaların karantina altına alınması, eklentinin çıkartılıp epostanın kullanıcıya gönderilmesi, vb. gibi farklı aksiyonları desteklemelidir.

1.10. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üzerinde, sisteme yönlendirilen e-postalarda bulunan virüs ve diğer zararlı yazılımları tespit eden bir tehdit tarama motoru bulunacaktır.

1.11. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üzerinde, sisteme yönlendirilen e-postalarda bulunan URL'leri tespit etmek amaçlı çevrim içi güncellemeye sahip bir URL filtreleme motoru bulunacaktır.

1.12. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üzerinde, epostaya bağlı gelen PDF/MHT/RTF tipindeki eklentiler içerisinde geçebilecek zararlı URL'leri tespit özelliğine sahip olmalıdır.

1.13. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi üzerinde, diğer motorlar tarafından tanımlanamayan ancak şüpheli görülen e-posta eklentilerinin izole bir ortamda derinlemesine analiz edileceği kum havuzu (sandbox) olarak adlandırılan sanal bilgisayar sistemi bulunduracaktır.

1.14. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üzerinde aynı anda çalışan en az 30 (altmış) kum havuzu makinesi desteği olacaktır.

1.15. Tekilf edilecek Gelişmiş Saldırı e-posta Analiz ve Engelleme Sistemi, üzerinde aynı anda çalışabilen 3 (üç) farklı kum havuzu (sandbox) makinesi desteği olacaktır.

1.16. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi ile e-Posta eklerinde

bulunabilecek,"pdf,exe,cmd,bat,ps1,doc,docs,svg,swf,mov,htm,html,xht,html,jar,class,dot,dotx,pps,ppsx,ppt,pptx,pub,xla,xls,xlsx,xlt,xlm,cell,xml,xlsb,xltx,hwp,hwpx,jtd,gul,msg,slk,jqy,csv,docm,dotm,potm,ppam,ppsm,pptm,xlam,xlsm,xltm,chm,lnk,rtf,js,jse,hta,vbe,vbs,wsf,url,cpl,crt,dll,drv,ocx,scr,sys,jqy" tipinde objeler analiz edilebilir olacaktır.

1.17. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, sıkıştırılmış dosyaları açılabilmeli ve içindeki dosyaların analizi gerçekleştirilebilmelidir. Sıkıştırılmış dosya formatı olarak, "*7z,ace,amg,arj,hqx,bz2,bzip2,cab,cpio,cpgz,gzip,gz,lha,lharc,lzh,eml,email,msg,rar,sit,sitx,tar,tgz,tnef,winmail.dat,win.dat,uue,xz,zip*" formatlarını desteklemelidir. Eğer sıkıştırılmış dosyalar şifre ile korunuyor ise yönetim arayüzü üzerinde şifrelenmiş dosyaları açmak üzere şifrelerin girilebileceği bir ekran sağlanmalıdır.

1.18. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, bulduğu zararlı e-postlar ile ilgili her türlü bilgiyi (mesaj içeriği, eposta ekran görüntüsü, mesaj başlıkları vb.) tutabilmeli, gerektiğinde detaylı analiz için dosyaların indirilmesine imkan verebilmelidir.

1.19. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üzerinde bulunan kum havuzu sistemi aşağıda listelenen özelliklere sahip olacaktır:

1.19.1. Kum havuzu sanal bilgisayarı kurum tarafından özelleştirilebilmeli ve sanal makine ayarları üzerinde kullanıcının ön gördüğü değişiklikler yapılabilmelidir.

1.19.2. Vmware, Hyper-V ya da Virtualbox standardında sanal makine standartlarını veya bu standartlarda oluşturulmuş sanal makinelerin otomatik çevirimlerini desteklemelidir.

1.19.3. Sanal makine olarak aşağıdaki işletim sistemleri desteklenmelidir:

1.19.3.1. Microsoft Windows XP 32-bit
1.19.3.2. Microsoft Windows XP 64-bit
1.19.3.3. Microsoft Windows 7 32-bit
1.19.3.4. Microsoft Windows 7 64-bit
1.19.3.5. Microsoft Windows 8 32-bit
1.19.3.6. Microsoft Windows 8 64-bit
1.19.3.7. Microsoft Windows 10 32-bit
1.19.3.8. Microsoft Windows 10 64-bit
1.19.3.9. Microsoft Windows Server 2003
1.19.3.10. Microsoft Windows Server 2008
1.19.3.11. Microsoft Windows Server 2012
1.19.3.12. Microsoft Windows Server 2016

1.19.4. Sanal makine olarak Türkçe Microsoft Windows tabanlı işletim sistemlerinin kullanımını desteklemelidir.

1.19.5. Kum Havuzu sistemi mimarisi içerisinde 50 (elli) MB'a kadar olan dosyaların analizine olanak sağlamalıdır.

1.19.6. Mobil işletim sistemlerini hedefleyen zararlı yazılımların da tespitini yapabilmelidir.

1.19.7. Mail içeriğinde bulunan URL'lerin işaret ettiği çalıştırılabilir dosyaların indirilmesi ve analiz edilebilmesi desteklenmelidir.

1.20. Teklif edilecek her bir Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üzerinde günlük ortalama 400.000 (dörtyüzbin) e-posta analiz edilebilmelidir.

1.21. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, internet üzerinden gerçek zamanlı güvenlik istihbarat bilgisi alabilecek, isteğe bağlı olarak da bu sisteme anonim saldırı istihbaratı verilerini iletebilecek olup bu özellik istenmediği durumda arayüz üzerinden kapatılabilecektir. Bu özellik için ayrı bir lisanslama bedeli teklif edilmeyecektir.

1.22. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, endüstri standardı güvenlik bilgi ve olay yönetim (SIEM) yazılımlarından HP ArcSight, IBM QRadar ve Splunk sistemleri ile entegre edilebilecektir.

1.23. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, zararlı olarak bulunan IP/Domain/URL bilgilerini, diğer güvenlik ürünleri ile paylaşabilmelidir (PaloAlto Fw, CheckPoint Fw, BlueCoat SG, TippingPoint IPS).

1.24. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, kullanıcı "manual submission" yöntemi ile verilen .eml uzatılı epostaları tarayabilecektir.

1.25. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi "*Machine Learning*" teknolojisi ile imza bağımsız olarak zararlıları tespit edebilecektir.

1.26. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, "Time-of – Click" özelliği ile izin verdiği bir URL'nin ileri bir tarihde erişilmek istendiğinde tekrar denetlenmesi için "rewrite" yöntemini destekleyecektir.

1.27. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi YARA kurallarını destekleyecektir.

1.28. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, repütasyon bazlı gelen epostaları gönderici IP adresine göre bloklayabilecektir.

1.29. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi , DHA (Directory Harvest Attack) Protection, Bounce Attack Protection özelliklerine sahip olacaktır.

1.30. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, eposta içeriğini inceleyerek anti-spam koruması sağlayacaktır.

1.31. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, ekli dosya tipi, dosya adı, dosya boyutu , dosya sayısı ve anahtar kelime gibi kriterlere göre slime, karantinaya alma, taglama aksiyonlarını alabilecektir.

1.32. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, "Social Engineering Attack Protection" özelliği ile sosyal mühendislik çabalarını algılayan ayrıca bir motora sahip olmalıdır.

1.33. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, oluşturulacak kural ve politikalarla, e-posta yolu ile gönderilebilecek içerikleri kontrol ederek engelleme özelliğine sahip olmalıdır.

1.34. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, Microsoft Office dosyalar içerisindeki aktif içerikleri (örnek: Macro) temizleyebilme özelliğine sahip olmalıdır.

1.35. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, üreticisi tarafından sunulan eposta saygınlık sistemi veri tabanına göre epostaların spam olup olmadığını sorgulayacak ve bu duruma göre aksiyonlar alınmasını sağlayabilecektir.

1.36. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, belli kişilerden gelen e-postlarda, içerik filtreleme, dosya engelleme gibi fonksiyonları gerçekleştirebilmelidir.

1.37. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, son kullanıcı karantina özelliğine sahip olmalı, kullanıcıların, karantinaya alınan e-postaları,

görüntüleyebilmesine, karantinadan çıkartabilmesine, silebilmesin olanak verecek şekilde çalıştırılabilmelidir.

1.38. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, taklit ve oltama yöntemlerine karşı SPF, DKIM ve DMARC yöntemlerini destekleyecektir. Ayrıca giden epostalar için DKIM imzalama yeteneği olacaktır

1.39. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme Sistemi, görünen dosya uzantısından bağımsız (true file type) olarak gerçek dosya tipini algılayarak silme, karantinaya alma, değiştirme gibi aksiyonlar alabilmelidir.

1.40. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme sistemi, izin verdiği epostaları, yük dengeleme ve önceliklendirme yöntemleri ile birden fazla eposta sunucusuna yönlendirebilecektir.

1.41. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme sistemi, LDAP sorgulaması ile alıcı adresi doğrulaması yapabilecektir ve alıcısı dizinde var olmayan epostaları reddedebilecektir.

1.42. Teklif edilecek Gelişmiş Saldırı e-Posta Analiz ve Engelleme sistemi 251 kullanıcı için 3 yıl olarak lisanslanmalıdır.

1.43. Teklif veren firma Teklif edilen Gelişmiş Saldırı e-Posta Analiz ve Engelleme sistemini yerinde kurumun istediği şekilde kurup yapılandıracaktır.

1.44. E-POSTA GÜVENLİK ÇÖZÜMÜ TEKNİK ŞARTNAMESİ

1.44.1. Teklif edilecek e-posta ağ geçidi yazılımı aşağıdaki özelliklere sahip olacaktır.

1.44.1.1. Teklif edilecek E-Posta Güvenlik Yazılımı, SMTP ağ geçidi ürünü olacaktır.

1.44.1.2. Teklif edilecek SMTP ağ geçidi yazılımı takip eden maddelerde sayılan özelliklere sahip olacaktır.

1.44.1.3. Teklif edilecek SMTP ağ geçidi sanal sunucular üzerinde ya da daha önceden uyumluluğu üretici tarafından belgelendirilmiş sunucu donanımları üzerinde çalışabilmelidir. Aşağıda belirtilen sanal sistemler desteklenmelidir.

1.44.1.3.1. Microsoft™ Windows Server 2008 R2 Service Pack 1 with Hyper-V

1.44.1.3.2. Windows Server 2012 with Hyper-V

1.44.1.3.3. Windows Server 2012 R2 with Hyper-V

1.44.1.3.4. Microsoft Hyper-V Server 2008 R2 SP1

1.44.1.3.5. Microsoft Hyper-V Server 2012 R2

1.44.1.3.6. VMware ESXi 5.0 Update 3

1.44.1.3.7. VMware ESXi 5.5 Update 2

1.44.1.3.8. VMware ESXi 6.0

1.44.1.4. Teklif edilecek SMTP ağ geçidi istenmeyen elektronik postalara (spam), virüslere ve zararlı yazılımlara karsı ağ geçidi olarak koruma sağlayacaktır.

1.44.1.5. Teklif edilecek SMTP ağ geçidi, LDAP sorgulaması ile alıcı adresi doğrulaması yapabilecektir ve alıcısı dizinde varolmayan epostaları reddedebilecektir.

1.44.1.6. Teklif edilecek SMTP ağ geçidi aşağıda belirtilen LDAP dizin sistemlerini desteklemelidir. LDAP sunucuları ile yapılan bağlantı SSL protokolü üzerinden gerçekleşmelidir (LDAP over SSL).

1.44.1.6.1. IBM Lotus Domino

1.44.1.6.2. Microsoft Active Directory

1.44.1.6.3. Microsoft AD Global Catalog

1.44.1.6.4. OpenLDAP

1.44.1.6.5. Sun iPlanet Directory

1.44.1.7. Teklif edilecek SMTP ağ geçidi, gönderici alan adı için DNS sorgusu yaparak DNS kaydı olmayan epostaları engelleyebilecektir

1.44.1.8. Teklif edilecek SMTP ağ geçidi, gönderici IP adresi için PTR sorgusu yapabilecektir ve PTR kaydı olmayan epostaları engelleyebilecektir.

1.44.1.9. Teklif edilecek SMTP ağ geçidi, izin verdiği epostaları, yük dengeleme ve önceliklendirme yöntemleri ile birden fazla eposta sunucusuna yönlendirebilecektir.

1.44.1.10. Teklif edilecek SMTP ağ geçidi, TLS destekleyecektir. Gelen bağlantılarda TLS protokolünü hem opsiyonel hem zorunlu olarak kullanabilecektir.

1.44.1.11. Teklif edilecek SMTP ağ geçidi Anti Spam ve Anti virüs özelliği ile teklif edilecektir.

1.44.1.12. Teklif edilecek SMTP ağ geçidi gelen ve giden tüm trafiği tek bir sanal sunucu üzerinde tarayabilmelidir.

1.44.1.13. Teklif edilecek SMTP ağ geçidi 0 gün virüs koruması ile şüpheli bulunan mesaj ekleri virüs karantinasına gönderilebilmelidir.

1.44.1.14. Teklif edilecek SMTP ağ geçidi ile Pazarlama, Sosyal Medya siteleri gibi yerlerden gelen e-postalar için ayrı bir filtreleme mekanizması bulunmalıdır. Bu mekanizmaya uygun şekilde kurallar yazılarak aksiyonlar alınması sağlanabilmelidir.

1.44.1.15. Teklif edilecek SMTP ağ geçidi üreticisi tarafından sunulan eposta saygınlık sistemi veritabanına göre epostaların spam olup olmadığını sorgulayacak ve bu duruma göre aksiyonlar alınmasını sağlayabilecektir.

1.44.1.16. Teklif edilecek SMTP ağ geçidi oltalama saldırılarına karşı Sosyal Mühendislik saldırılarından koruma yeteneğine sahip olmalıdır.

1.44.1.17. Teklif edilecek SMTP ağ geçidi Spyware, adware tipinde zararlılara karşı koruma sağlamalıdır.

1.44.1.18. Teklif edilecek SMTP ağ geçidi, giden e-postalar için DKIM imzalama metodunu (DomainKeys Identified Mail Signing) desteklemelidir.

1.44.1.19. Teklif edilecek SMTP ağ geçidi, SPF(Sender Policy Framework) doğrulaması yapabilecektir. Bu doğrulama sonucuna göre reddetme, karantinaya alma ve benzeri aksiyonlar alabilecektir.

1.44.1.20. Teklif edilecek SMTP ağ geçidi uyumlu bir Internet tarayıcısı ile yönetilebilecek HTTPS tabanlı bir web yönetim arayüzüne sahip olmalıdır.

1.44.1.21. Yönetim arayüzü üzerinde; sistem bileşenlerinin güncellik derecesi, anlık olarak işlemci, hafıza, disk kullanımı, sistem tarafından denetlenen ve yakalanan zararlı mail istatistikleri gibi bilgiler görülebilmelidir.

1.44.1.22. Teklif edilecek SMTP ağ geçidi gelen e-posta içeirsinde bulunan linkleri gerçek zamanlı bir reputasyon filtresinden geçirerek zararlı linkler bulunduran e-postaları engelleyebilmeli, karantina altına alabilmelidir.

1.44.1.23. Teklif edilecek SMTP ağ geçidi, e-posta içerisinde geçen URL adresleri o anda veritabanında zararlı olarak işaretlenmemiş olsa dahi ilerde zararlı olarak veritabanına eklenmesi ihtimaline karşı URL adresinin hedefini değiştirerek izin verebilmelidir. Böylece kullanıcının ileri bir tarihte URL adresine gidişini engelleyebilmelidir.

1.44.1.24. Teklif edilecek SMTP ağ geçidi gelen ve giden e-postalara boyut ve gönderici sayısı sınırlamaları uygulayabilmelidir.

1.44.1.25. Teklif edilecek SMTP ağ geçidi, aşağıda belirtilen son kullanıcı karantina özelliklerini sağlamalıdır.

1.44.1.25.1. Son Kullanıcı Karantina Sistemi (EUQ), doğrulama sistemi içermelidir. Doğrulama sistemi, LDAP dizin sistemini ve SMTP doğrulama sistemini desteklemelidir.

1.44.1.25.2. Son Kullanıcı Karantina Sistemi (EUQ), günlük olarak kullanıcılara karantina bilgilendirme e-postası iletebilmelidir.

1.44.1.25.3. Son Kullanıcı Karantina Sistemi (EUQ), kullanıcılara web tabanlı bir arayüz üzerinden karantinaya alınan e-postaların yönetimini desteklemelidir.

1.44.1.25.4. Son Kullanıcı Karantina Sistemi (EUQ) üzerinden gönderilen bilgilendirme e-postaları içerisinde karantinaya alınmış e-postalar için silme ya da karantinadan çıkarma aksiyonlarına dair linkler bulunmalıdır.

1.44.1.26. Teklif edilecek SMTP ağ geçidi istendiğinde internette ön filtreleme yaparak sisteme gereksiz e-posta gelmesini önleyebilir özellikte olmalıdır. İnternette yapılacak ön filtreleme ayarları SMTP ağ geçidi üzerinden tanımlanmalıdır. Bu özellik isteğe bağlı olarak açılıp kapatılabilmelidir.

1.44.1.27. Teklif edilecek SMTP ağ geçidi görünen dosya uzantısından bağımsız olarak gerçek dosya tipini algılayarak silme, karantinaya alma, değiştirme gibi aksiyonlar alabilmelidir.

1.44.1.28. Teklif edilecek SMTP ağ geçidi üzerinde şifre korumalı taranamayan ekler için özel politika tanımlanabilmelidir.

1.44.1.29. Teklif edilecek SMTP ağ geçidi şifre korumalı sıkıştırılmış ZIP dosyalarının içindeki dosyaları algılayarak bu dosyalar için isim ve uzantıya göre bloklama politikası uygulayabilmelidr.

1.44.1.30. Teklif edilecek SMTP ağ geçidi, sıkıştırılmış dosyalarda (ZIP, ARJ,LZH, RAR, TAR, CAB,TD0,7Z, BZ2, VBX) zararlı denetimi yapabilecektir.

1.44.1.31. Teklif edilecek SMTP ağ geçidi, kendi üzerinde bulunan olay kayıtlarını syslog entegrasyonu ile birden çok kaynağa iletebilmelidir.

1.44.1.32. Teklif edilecek SMTP ağ geçidi, sıkıştırılmış dosyalarda birden fazla iç içe katman olarak sıkıştırılmış dosyaları açabilecek ve denetim yapabilecektir.

1.44.1.33. Teklif edilecek SMTP ağ geçidi, mail bombardımanlarını algılayıp engelleme yapabilecektir.

1.44.1.34. Teklif edilecek SMTP ağ geçidi, göndericinin mail adresi ya da IP adresine göre izin verilen ya da engellenen liste kurallarını uygulayabilmelidir.

1.44.1.35. Teklif edilecek SMTP ağ geçidi, e-posta başlığına, içeriğine ve eklentisine göre filtre tanımlanmasına imkan tanımalıdır.

1.44.1.36. Teklif edilecek SMTP ağ geçidi, anti-spoofing özelliği barındırmalıdır.

1.44.1.37. Teklif edilecek SMTP ağ geçidi, gövde filtreleme (body filter) desteği olmalıdır.
1.44.1.38. Teklif edilecek SMTP ağ geçidi, anahtar sözcük bazında e-postanın ekinin içeriği kontrol edilebilmelidir.
1.44.1.39. Teklif edilecek SMTP ağ geçidi, e-posta içindeki kötü niyetli URL'lere karsı koruma sağlamalıdır.
1.44.1.40. Teklif edilecek SMTP ağ geçidi, e-posta eklerini spam ve virüs içeriğe karşı kontrol edebilmelidir.
1.44.1.41. Teklif edilecek SMTP ağ geçidi, spam olarak tespit edilen e-postaları silebilmeli, başka bir adrese gönderebilmeli, karantinada tutabilmeli, konu kısmına, e-posta bölümüne özel bir mesaj ekleyebilmelidir.
1.44.1.42. Teklif edilecek SMTP ağ geçidi, belirli bir ip adresinden gelen bağlantı sayısı önceden tanımlanmış maksimum bağlantı değerini aştığında, kaynak ip adresini bloklamayı desteklemelidir.
1.44.1.43. Teklif edilecek SMTP ağ geçidi, belirli bir e-posta adresinden gelen eposta sayısı önceden tanımlanmış maksimum eposta değerini aştığında, kaynak eposta adresini bloklamayı desteklemelidir.
1.44.1.44. Teklif edilecek E-posta ağ geçidi, Gelişmiş Saldırılar için Detaylı Analiz Sistemi ile entegre olabilecek, gelen e-postaları analiz amacı ile bu sisteme iletebilecektir.
1.44.1.45. Teklif edilecek E-posta ağ geçidi, Gelişmiş Saldırılar için harici bir Detaylı Analiz Sistemi ile entegrasyonu ile zararlı içerik bulunduran e-postaları Detaylı Analiz Sistemi bulgularına uygun şekilde karantinaya alabilecektir.
1.44.1.46. Teklif edilecek E-Posta Güvenlik Çözümü 251 kullanıcı için 3 yıl olarak lisanslanmalıdır.
1.44.1.47. Teklif veren firma Teklif edilen E-Posta Güvenlik Çözümünü yerinde kurumun istediği şekilde kurup yapılandıracaktır.