Sabancı Üniversitesi Firewall Alımı Teknik Şartnamesi

1. Firewall Teknik Özellikleri

1.1. Harici anahtar (switch), yük dengeleyici, orkestrator gibi donanımlar ile sağlanan cluster/küme/dağıtık mimarideki çözümler kabul edilmeyecektir.

1.2. Bu şartnamede belirtilen özelliklerin tümünü sağlayan bir çift güvenlik duvarı yedeklilik yapılandırması ile teklif edilecektir. Aktif güvenlik duvarı ve yedek cihaz aynı ürün modeli olacaktır. Aktif cihazda bir sorun oluşması durumunda tüm trafik kesintisiz ikinci cihazdan devam edecektir.

1.3. Mevcut firewall cihazlarından politika geçişlerini ve kural optimizasyonlarını yapacak servis ve yazılımlar ücretsiz olarak sağlanacaktır. Bu servisler ile uygulamaya göre yazılmamış kurallar uygulamaya çevrilecek, uygulama kurallarında ise kullanılmayan uygulamalar tespit edilerek kaldırılacaktır. Bu işlemler için mevcut kurallardan en az 30 gün süre ile geçen uygulamalar ve bu uygulamalardaki trafik miktarları görüntülenecek ve aynı ekrandan uygulamalar kurala eklenebilecektir. Bu servis ve yazılımlar 5 yıl süre ile kurum tarafından kullanılabilecektir. Bu sayede düzenli kontroller ile kurumdaki güvenlik politikalarının uygulama ve kullanıcı entegrasyonları ile kural sıkılaştırmaları yapılabilecektir. Lisans gerekiyorsa bu servisler için teklife dâhil edilecektir.

1.4. Teklif edilecek cihazların tüm teknik özellikleri ve detayları üreticinin herkese açık web sayfasında ihale tarihi itibarı ile yayınlanmış olması gerekmektedir. Dolayısı ile ürün dokümanında hedef performans değişime tabidir gibi belirsizlikler yer almayacaktır. İlgili ürün ihale tarihinde kuruma sipariş edilebilir konumda olacaktır.

1.5. Teklif edilen güvenlik duvarı çözümünün işletim sistemi update, hotfix install, lisanslama, imza veritabanı güncelleme gibi tüm işlemleri arayüzünden yapılabilecektir.

1.6. Cihazın kendi web yönetim ara yüzü üzerinden kural değişiklikleri güvenlik duvarına yüklenirken aktif kurallar otomatik olarak yedeklenebilecektir.

1.7. Cihaz üzerinde ya da dışarıya export edilen kurallar ve cihaz konfigürasyonu yeniden başlatmaya ihtiyaç duymadan geri yüklenebilecektir.

1.8. Cihaz üzerindeki uygulama imzaları, IPS imzaları ve antivirüs imzaları cihazın hiçbir internet bağlantısı olmaması durumunda dahi herhangi bir ek yazılıma gerek duymadan cihazın kendi web arayüzü üzerinden dosya yükleme yöntemi ile kullanıcı tarafından güncellenebilecektir.

1.9. Teklif edilen güvenlik duvarı bu şartnamede talep edilen özellikler aktif ve kullanılırken kurumun kritikliği nedeni ile TCP sync ataklara karşı efektif bir korumaya sahip olacaktır. Bu kapsamda güvenlik duvarı üzerindeki bir ya da birden fazla interface üzerindeki ip adresine flood TCP sync paketleri geldiğinde belirlenecek olan saniyelik connection değerleri doğrultusunda koruma sağlanacaktır.

1.10. Teklif edilecek cihaz DHCP server, DHCP Client ve DHCP Relay yeteneğine sahip olacaktır.

1.11. Sistem statik ve Dinamik (OSPFv2/v3, BGPv4, RIPv2) Yönlendirme protokollerine sahip olacaktır.

1.12. Güvenlik Duvarı BFD (Bidirectional Forward detection) özelliğine sahip olmalıdır. Böylece yönlendirme seviyesinde oluşabilecek herhangi bir değişiklikte daha hızlı adaptasyon sağlanabilecektir.

1.13. Cihazın Multicast yönlendirme desteği olmalı ve PIM-SM, PIM-SSM, IGMP v1, v2, v3 desteklemelidir.

1.14. Teklif edilen ürün aktif/pasif çalışabilme yeteneğine sahip olacaktır.

1.15. Teklif edilecek cihaz ASIC, FPGA yada ssl decryption performansı arttırmak için Integrated Crypto Assistant mimariye sahip olacaktır.

1.16. Teklif edilecek sistemler destekledikleri maksimum RAM ve bellek ile teklif edilecektir.

1.17. Cihaz üzerinde en az 1 (bir) adet sanal firewall oluşturulması için gerekli lisanslar teklife dahil edilecektir. Ek lisans ile sistem en az 10 adet sanal firewall kadar genişleyebilecektir.

1.18. Teklif edilecek her bir cihaz üzerinde en az 12 (on iki) adet 1G/2.5G/5G/10G Gbps hızında RJ45 bakır (10 adet 10G bakır aynı anda kullanılabilmelidir), bunun yanında en az 10 (on) adet 1/10 (bir/on) Gbps hızında SFP/SFP+ fiber, en az 4 (dört) adet 25 Gbps hızında SFP28 fiber veri portu olacaktır. Sistem üzerinde bu portların tümü aynı anda kullanılabilecektir.

1.19. Bu şartnamede talep edilen veri portları haricinde HA yapısı için en az 2 (iki) adet 1Gbps BASE-T ve 1 (bir) adet SFP+ fiber portlar olacaktır. Bu portlar iki cihazın HA bağlantısı ve session senkronizasyonu için kullanılacaktır.

1.20. Teklif edilecek her bir cihaz üzerinde yönetim için kullanılacak en az 1 (bir) adet 1 Gbps RJ45 portu bulunacaktır.

1.21. Teklif edilecek cihazın SSL Decyrption değeri aşağıdaki kriterlerin üzerinde olacaktır. SSL decryption sırasında Threat Prevention/Detection açık olacak ölçümlenecektir. Bu değer için minimum protokol, cipher ve şifreleme anahtar boyutları aşağıdaki gibi olacaktır.

1.21.1. Bağımsız test kuruluşuna ait bir veri, ya da kurumun kendi test imkanları ile bu değerlerin ölçümlenmesi sırasında 64B statik payload'a sahip http Get/Response ile ölçeklendirilmiş Threat Prevention/IPS, URL Filtering, Anti Virus/Anti Spyware, Data/File Blocking&Filtering, E-mail filtering ve Zero Day Atak koruma önlemleri açık olarak tutularak yapılmalıdır. Trafik paterni ve ilgili çıktılarını teklif ile birlikte paylaşacaktır.

TLS version	Cipher Suites	Throughput (Gb/s)
1.2	ECDHE-AES-256- SHA-384	>2.3
1.3	AES-256-SHA-384 4K Key	>2.0

1.22. Teklif edilecek cihazın Atak Önleme (Threat Prevention) throughput değeri en az 8.5 Gbps performansına sahip olacaktır. Bu değer Application Control, IPS, Anti-Virüs, Anti-spyware, Zero Day Saldırıları (APT) Tespit ve Analiz, DNS Security, File Blocking ve cihaz üzerinde loglama özellikleri aynı anda açık iken appmix/entmix değerleri ile sağlanacaktır. Bu değerler üreticinin herkese açık dokümanlarında madde de yer alan özelliklerin tümü aktifken açıkça belirtilmiş olacaktır.

1.23. Teklif edilecek cihazın L7 seviyesinde Güvenlik Duvarı (Firewall) throughput değeri az 16 Gbps performansına sahip olacaktır. Bu değer appmix/entmix olarak uygulama kontrolü ve loglama açıkken sağlanacaktır. Bu değerler üreticinin herkese açık dokümanlarında madde de yer alan özelliklerin tümü aktifken açıkça belirtilmiş olacaktır.

1.24. Teklif edilecek cihaz anlık olarak en az 2.000.000 (iki milyon) oturum kapasitesine sahip olacaktır.

1.25. Threat Prevention/IPS, URL Filtering, Anti Virus/Anti Spyware, Data/File Blocking&Filtering, E-mail filtering ve Zero Day Atak koruma önlemleri açık iken eş zamanlı TCP oturum sayısı en az 1.500.000 (bir milyon beş yüz bin) olmalıdır. Bağımsız test kuruluşuna ait bir veri, ya da kurumun kendi test imkanları ile 1Byte'lık http 1.1 payload'u kullanarak sıkıştırma kullanmadan test ederek, trafik paterni ve ilgili çıktılarını teklif ile birlikte paylaşacaktır.

1.26. Teklif edilecek cihaz saniyede en az 200.000 (iki yüz bin) yeni oturum açabilme kapasitesine sahip olacaktır.

1.27. Teklif edilecek cihaz üzerinde son kullanıcı ağları arası trafik geçişi ve trafik yönlendirme yapılacağından arp tablosu en az 12.000 kayıt tutabilecektir.

1.28. Teklif edilen cihazlar yedeklilik için birbirleri ile doğrudan en az bir adet olarak 10 Gbps SFP+ port üzerinden bağlanacaktır. Yedeklilik mimarisi herhangi bir ek donanım ihtiyaç olmadan doğrudan cihaz üzerinden yapılacaktır.

1.29. Teklif edilecek cihaz üzerindeki tüm güç kaynağı yuvaları tamamen dolu olarak teklif edilecektir.

1.30. Teklif edilecek cihaz üzerinde 480GB SSD disk olacaktır. Bu disk işletim sistemi ve loglama için kullanılacaktır.

1.31. Teklif edilecek cihaz kendi üzerindeki Web tabanlı arayüzü üzerinden yönetilebilecektir. Bu web arayüzü üzerinden sadece cihaz sistem ayarları değil güvenlik politikası ekleme, güncelleme gibi tüm işlemler de yapılabilecektir.

1.32. Teklif edilecek güvenlik duvarları aşağıdaki servislere sahip olmalı ve bunlar için gerekli lisanslar teklife dahil edilmelidir.

1.32.1. Güvenlik Duvarı
1.32.2. NAT ipv4, NAT ipv6 ve NAT64
1.32.3. Site-to-site IPSEC VPN
1.32.4. Remote/Client için SSL VPN ya da IPSEC VPN
1.32.5. Uygulama kontrolü (Application Control)
1.32.6. Saldırı Engelleme (IPS)
1.32.7. Anti-Virus
1.32.8. Anti-Bot ya da Anti-Spyware
1.32.9. URL Filtreleme ve güvenlik kontrolü
1.32.10. Dosya uzantısına göre upload ve download yönünde kontrol
1.32.11. Kullanıcı kimliği entegrasyon özelliği
1.32.12. SSL çözme ve yönlendirme
1.32.13. Band genişliği kontrolü (QoS)

1.33. Güvenlik Duvarı LLDP (Link Layer Discover Protocol) protokolünü desteklemelidir. Böylece cihaz kendine bağlı diğer cihazlar ile ilgili bilgileri (Mac adresi, sistem adı, kendine bağlı port ile ilgili bilgileri) sunabilmelidir.

1.34. Path monitoring özelliği cihaz üzerinde tanımlanan statik route tanımları bağdaştırılabilecektir. Böylece tanımlanan statik yönlendirmeler üzerinden sağlanan erişimlerin çalışıp çalışmadığını kontrol edebilecektir. Erişim olmadığı durumlarda statik

yönlendirme satırını yönlendirme tablosundan otomatik olarak kaldırarak alternatif yoldan erişim imkânı sağlanacaktır.

1.35. Uzak kullanıcılar için ajan ile SSL VPN özelliği, Windows PC, MACOS tabanlı istemcileri desteklemelidir. En az 1800 adet ajanlı SSL VPN client sisteme bağlanabilmelidir.

1.36. Cihazın yeniden başlatılmasına gerek kalmadan üzerindeki portların çalışma seviyesi (L2, L3, monitoring) istendiği gibi değiştirilebilmelidir.

1.37. Teklif edilecek cihaz üzerinde aynı fiziksel ya da sanal Layer-3 arayüz için birden fazla ip adresi tanımlanabilecektir. Bu ip adresleri NAT ve routing işlemleri dahil olmak üzere aktif olarak kullanılabilecektir.

1.38. MS Active Directory ile entegre olarak kişi ve grup bazında kural yazılabilecektir. Kullanıcıya göre kural yazma sadece kimlik bilgisi gönderen uygulamalarla sınırlı olmayacaktır. Tutulan kayıtlarda kullanıcı ismi de yer alacaktır.

1.39. Yeni Nesil Güvenlik Duvarı terminal server yapısında birden fazla kullanıcının bağlanarak ilgili terminal sunucu ip adresi ile gerçekleştirdiği trafiklerden kullanıcı adı ve ip eşleştirmesi yapabilmelidir. Bu durumda terminal sunucu üzerindeki her bir kullanıcı için belirli bir port sayısı allocate edilebilmeli ve buna göre agent desteklediği anlık kullanıcı sayısı dinamik olarak güncellenebilmelidir.

1.40. Teklif edilecek cihaz, bu şartnamede yer alan özellikleri aktifken kimlik denetimini kendi üzerinde yapılandırılmış lokal veri tabanına ek olarak özellikle MFA entegrasyonları için Radius ve SAML üzerinden yapabilmelidir. Sistem üzerinde yetkilendirilen kullanıcılara farklı roller atayabilmelidir.

1.41. Teklif edilecek cihaz kendi üzerindeki loglarda kullanıcı tarafından oluşturulacak filtreler ile ip adreslerini ve kullanıcı isimlerini işaretleyerek, bunları güvenlik kurallarında dinamik olarak kullanabilecektir. Bu işlemde bir kez tag (işaret) oluşturularak dinamik grup/nesne güvenlik kurallarına eklendiğinde, loglarda filtreye uygun olan nesne otomatik olarak ilgili gruba eklenecek ve güvenlik kuralında aktif olacaktır.

1.42. Teklif edilecek cihazların Data filtreleme özelliği olacak ve kural tabanlı çalışacaktır. Dosya türü, keyword, regex özelliklerini sağlamalıdır. Bunun için gerekli lisanslar teklife dahil edilecektir.

1.43. Yeni Nesil Zero Trust yaklaşımı ile mümkün olan en iyi seviyede ve fazla sayıda uygulamanın tanınabilmesi ve güvenlik kurallarının bu şekilde kullanılabilmesi için cihaz üzerinde en az 3500 uygulamayı tanıyabilen uygulama kontrol özelliği olacaktır.

1.44. Farklı kullanıcı veya kullanıcı grupları için farklı IPS politikaları oluşturulabilmelidir.

1.45. Önerilecek IPS fonksiyonunda saldırı imzalarına bağımlı kalmaksızın saldırıları engelleyen Protokol Anormallik Tespiti (Protocol Anomaly Detection) teknolojisine sahip olacaktır.

1.46. Cihaz üzerinde Anti-Spyware tespit ve engelleme özelliği olmalıdır.

1.47. Anti-Spyware özelliği ile port ve protokolden bağımsız, internete doğru yapılan tüm ip trafiğini inceleyebilmelidir.

1.48. Botnet komuta kontrol merkezlerine erişim için yapılan adres çözümleme isteklerini tespit ve dns sorgusu esnasında trafiği bloklayabilme ve özelliğine sahip olmalıdır.

1.49. Sıfırıncı gün ataklara karşı koruma sağlama özelliği olacaktır ve lisanslar eklenecektir.

1.50. Cihazın DNS Sinkhole özelliği ile, kötü domain isteklerini yönetici tarafından atanmış IP adresine çözülmesini sağlayabilmelidir. Böylelikle sistem üzerinde enfekte olmuş sistemler kolyaca tespit edilebilecektir.

1.51. Bilinen botnet'ler için imza temelli bloklama yapabilmelidir. Her bir botnet imzası için alınabilecek aksiyonlar sistem yöneticileri tarafından konfigüre edilebilmelidir.

1.52. Farklı kullanıcı veya kullanıcı grupları için farklı antivirüs politikaları oluşturulabilmelidir.

1.53. Antivirüs özelliği en az HTTP, HTTP2, SMB, FTP, POP3 ve IMAP protokollerini tarayabilmelidir.

1.54. URL filtreleme özelliği Active Directory ile entegre çalışabilecek bu sayede Active Directory'de tanımlı olan kullanıcı ve kullanıcı grupları bazında URL filtreleme kuralları tanımlanabilecektir.

1.55. Güncel zararlı yazılımların eriştiği C&C (Command and Control) ve Malware Download URL listelerini dinamik olarak güncelleyebilmelidir.

1.56. URL filtreleme özelliğinde XFF (X-forwarded-for) özelliği bulunmalıdır.

1.57. URL filtreleme özelliği ile kategorize edilmemiş sitelere yapılan erişimler paralelinde sistem yöneticilerinin müdahalesi ile kategorizasyon yapabilme özelliği olmalıdır. Sistem yöneticisi, özel kara liste ve beyaz liste kategorileri oluşturabilmelidir.

1.58. URL filtreleme özelliği ile bulut mimarisi sayesinde bulut veritabanı üzerinde yapılan tüm güncellemelerden kurumun anında faydalanması mümkün olmalıdır.

1.59. URL filtreleme özelliği ile güncel zararlı yazılımların eriştiği C&C (Command and Control) ve Malware Download URL listelerini dinamik olarak güncelleyebilmelidir.

1.60. URL kategorileri üzerinde, kullanıcılara uyarı ekranı çıkarıp devam seçeneği ile devam etme (istemsiz dosya indirmelere karşı) ve override (sifre ile erişim) aksiyonları alınabilecektir.

1.61. Cihaz üzerinde URL kategorilerine göre özel güvenlik uygulamaya yönelik politikaları yazılabilecektir. Bilinmeyen/proxy kategorilerindeki URL ve sitelere web ile erişime izin verirken, dosya indirmeyi yasaklamak gibi aksiyonlar alınabilecektir.

1.62. URL kategorilerini kullanarak security policy match kısmında kullanılabilmeli ve her bir URL kategorisi için farklı bant genişliği sınırlandırma politikaları yazılabilmelidir.

1.63. Oltalama (phishing) saldırılarına karşı, kullanıcı kimlik bilgilerinin firma dışına çıkmaması için (User-id submission) kontrol özelliği olacaktır.

1.64. Cihazlar, SSL web tabanlı trafiği decrypt edebilmelidir. SSL decryption aktif iken, madde 1.22'de verilen trafik miktarlarında SSL trafiği TLS v1.2 ve v1.3 için karşılanmalıdır. Cihaz kendi üzerinde self-signed CA root sertifika üretebilecektir.

1.65. Inbound (giriş) ve Outbound (çıkış) yönünde HTTPS decryption yapabilecektir. TLS 1.2 ve TLS 1.3 decryption desteği olacaktır. TLS 1.3 trafiği, TLS 1.2 sürümüne downgrade edilmeyecektir. HTTP/2 uygulamaları için bütün kontrol özelliklerini kullanabilecektir. (App-control, IPS, AV, dosya bloklama vb). HTTPS trafiğinin incelenebilmesi için gerekli olan Sertifika Yeni Nesil Güvenlik Duvarına dışardan yüklenebilecektir. Aynı zamanda Yeni Nesil Güvenlik Duvarı üzerinde üretilen bir self-signed SSL sertifika da bu amaç için kullanılabilecektir. Yeni Nesil Güvenlik Duvarı kendi üzerinde self-signed CA root sertifika üretecektir.

1.66. Yeni Nesil Güvenlik Duvarı üzerindeki ataklara karşı üstün koruma için bölgesel koruma özelliği (zone protection) sayesinde IP, TCP, ICMP, IPv6 ve ICMPv6 için paket bazlı koruma değerleri tanımlanabilecektir. Bu değerler oluşturulan her bir bölge için ayrıca belirlenebilecek ve bu değerlerin aşılma durumları Yeni Nesil Güvenlik Duvarı üzerindeki loglarda gözlemlenebilecektir.

1.67. Yeni Nesil Güvenlik Duvarı üzerindeki kaynakları atak anında koruyabilmek ve normal trafiğin sorunsuz geçişine imkan tanımak için paket ön bellek (packet buffer) koruma özelliği bulunacaktır. Bu özellik ile paket işlemedeki gecikme parametrelerine ve packet buffer kullanım oranına göre koruma sağlanacaktır.

1.68. Coğrafi bölgelere (Geo IP) göre güvenlik kuralları uygulanabilecek, bir kurala birden çok coğrafi bölge eklenebilecektir.

1.69. Cihaz QoS destekleyecektir. Kullanıcı adı/grubu, hedef/kaynak IP, URL kategoriye göre ve uygulama bazında bant genişliği sınırlaması yapabilmelidir. Ayrıca Trafik önceliklendirme yapabilecektir. Cihaz DSCP marking yapabilecektir.

1.70. Cihaz Network Packet Broker ve SSL visibility tool olarak çalışabilecektir. Bu özelliğin desteklenmesi için ayrı bir lisans gerekli ise bu lisanlar da teklife dahil olacaktır. Eğer üretici bu özellikleri teklif edilen firewall cihazı üzerinde sağlayamıyorsa bu özellikleri sağlayan ayrı bir cihaz teklife eklenecektir.

1.71. Kural bazlı olarak TCP, UDP paketlerini farklı cihazlara gönderip alabilecektir. Zone, kaynak/hedef IP, Uygulama ve kullanıcı kimliği bazlı olarak paketleri farklı üçüncü taraf trafik işleme cihaz ya da sistemlerine (IPS, Network Forensic, Sandbox vb.) gönderebilmelidir.

1.72. Cihazlar, üzerine gelen istemci tabanlı ve sunuculara doğru gelen web SSL trafiğini decrypt edebilmeli ve decrypt ettiği bu trafiği üçüncü taraf trafik işleme cihaz ya da sistemlerine (IPS, Network Forensic vb.) in-line (Layer2) ve routed (Layer3) zincir olarak gönderebilmelidir. Bahse konu üçüncü taraf cihaz ya da sistemler, trafik üzerinde gerekli işlemleri gerçekleştirdikten sonra teklif edilecek cihazlar bu trafiği üçüncü taraf cihaz ya da sistemlerden geri alıp tekrar encrypt ederek trafiğin yoluna devam etmesini sağlayabilmelidir. Eğer üretici bu özellikleri teklif edilen firewall cihazı üzerinde sağlayamıyorsa bu özellikleri sağlayan ayrı bir cihaz teklife eklenecektir.

1.73. Cihaz üzerinde dinamik IP/URL/Domain adresi engelleme listeleri oluşturulabilecektir. Engellenecek IP adreslerinin listesinin tutulduğu URL den bu listeyi cihaz otomatik olarak alarak güvenlik duvarı üzerinde bu IP/URL/Domain adreslerin erişimini engelleyebilecektir.

1.74. Güvenlik duvarı üzerine eklenen dinamik listeler sayesinde en fazla 5 dakika süreli güncelleme ile en az 50.000 IP adresini, 1 Milyon domain kaydını ve en az 100.000 URL kaydını listelere çekebilecektir. Bu listeleri güvenlik kurallarında kullanabilecektir. Dinamik listelere yeni bir ip/url/domain kaydı güncellendiğinde bu işlem için commit/kural aktif etme gibi ek bir işleme gerek kalmayacaktır.

1.75. Güvenlik duvarı arayüzünden halihazırda gelen raporlara ek olarak, yeni taslak raporlar oluşturularak kurumun bildirdiği kişilere eposta yolu ile günlük/haftalık ya da aylık otomatik olarak iletilebilecektir.

1.76. Firewall üzerinde Torrent trafiği kesinlikle durdurulabilmedilir. İstenen IP ağı ve/veya kullanıcı grubuna göre whitelist yazılabilecektir.

1.77. Freeradius, dhcp ve diğer log kaynaklarından (Freeradius'tan kullanıcı adı ve MAC adresi, DHCP sunucudan MAC ve IP adresi) kullanıcıları ve IP adresleri eşleştirilebilmelidir.

1.78. Teklif edilen Ağ Güvenlik Duvarı Sistemi üreticisi, son 4 (dört) yıl için "Enterprise Firewall" "Gartner Magic Quadrant" tablosunda Liderler alanında yer almalıdır.

2. Kurulum ve Destek

2.1. Üniversitede şu an ayrı ayrı (kuralları farklı, cluster değil) çalışmakta olan 2 firewall mevcut kurulacak firewall çifti üzerinden çalışacak şekilde aktarılacaktır. Aktarım sırasında tüm firewall kuralları yeniden hesaplanarak korelasyonu yapılacaktır. Bu aktarım sırasında üniversite ağında OSPF ve default route tanımlarındaki değişiklikler kuran firma tarafından yapılacaktır.

2.1.1. Güvenlik duvarı geçişini yapacak olan kurum içerisinde teklif edilen güvenlik duvarı üreticisine ait en az 6 adet en üst düzey geçerli sertifikalı personel bulunduğunu kanıtlamalıdır.

2.1.2. Hibrit ağ donanımları olmasından dolayı, entegrasyonu üstlenecek kurum personeli dinamik routing protokollerindeki yetkinliğini kanıtlayacak expert seviyesindeki geçerli sertifikasını teklif ile birlikte üniversiteye sunacaktır.

2.1.3. İhtiyaç olması durumunda dinamik routing protokolünün migration hizmeti için ek bir ücret talep edilmeyecektir.

2.2. Veri merkezi üzerindeki Layer3 IP (SVI, RVI) ve ilgili VLAN'ler, yeni kurulacak Firewall üzerine aktarılacaktır.

2.2.1. Bu yeni ağların ilgili dinamik routing protokolü ile anonsları gerçekleştirilecektir.

2.2.2. Veri merkezindeki Layer3 anahtarlardaki ilgili interface ler altında bulunan erişim kontrol listelerine (ACL) ait tanımların firewall üzerine aktarılması sağlanacaktır.

2.3. Kurulacak Firewall'larda üretilen loglar, Üniversite syslog sunucusuna aktarılacaktır, aktarılan loglar günlük olarak arşivlenecektir. Syslog sunucuna aktarım sırasında gereksiz (üniversite yönetiminin belirlediği) log'lar filtrelenebilmelidir.

2.4. Üniversitenin 4 farklı lokasyonundaki pfsense güvenlik duvarlarından bu kurulacak Firewall'lara noktadan noktaya VPN bağlantısı yapılacaktır.

2.4.1. Bu lokasyonlara ait kural düzenlemeleri merkez güvenlik duvarı üzerinde yapılacaktır.

2.5. Bakım destek. 5 yıl boyunca firma desteği ve buna ait SLA değerleri (yılda uzaktan ve yakından ticket sayıları. Yüksek ve normal öncelikli çağrıların çözüm süreleri)

Çağrı önceliği	İlk müdahale	Çözüm süresi
Düşük	8 saat	4 gün
Orta	4 saat	1 gün
Yüksek	30 dak	6 saat

2.6. Kurulumdan sonra 2 günlük ürün kullanımına ait (kural yazma, os güncelleme, log inceleme, executive rapor üretme, top src/dst traffic IP, top connection IP vb) eğitim verilecektir.