**İŞ GEREKSİNİMLERİ DİYAGRAMI**

**Proje Konusu: Bilgi Sistemleri Güvenliği**

**Proje Adı: Bilgi Sistemleri Güvenliği için UTM Tabanlı Sistem Tasarımı ve Uygulaması**

1. Genel Gereksinimler

* Güvenlik Sistemi Entegrasyonu: Çeşitli güvenlik sistemlerinin UTM platformu altında birleştirilmesi. Tüm sistemlerin birbirleriyle uyumlu çalışması ve sürekli güncellenmesi.
* Merkezi Yönetim: Tüm güvenlik sistemlerinin tek bir yönetim noktasından izlenmesi ve yönetilmesi. Kullanıcı dostu bir yönetim arayüzü sağlanması.
* Uyumluluk ve Güncellemeler: Entegrasyon sürecinde uyumluluk sorunlarının minimize edilmesi. Sürekli güncellemelerin otomatik olarak uygulanabilmesi.

1. İşlevsel Gereksinimler

* Ağ Erişim Kontrolü (NAC): Sistem, kimlik doğrulama, yetkilendirme ve erişim kontrolü gibi NAC işlevlerini sağlayabilmelidir.
* Kullanıcı Kimlik Doğrulama: Sistem, kullanıcıların ağa erişmeden önce kimliklerini doğrulamalarını sağlayabilmelidir.
* Cihaz Kimlik Doğrulama: Sistem, cihazlara ağa erişim izni vermeden önce kimliklerini doğrulamalarını sağlayabilmelidir.
* Yetkilendirme: Sistem, kullanıcılara ve cihazlara ağda hangi kaynaklara erişebileceklerini belirleme imkanı sağlayabilmelidir.
* Erişim Kontrolü: Sistem, ağa yetkisiz erişimi önleyebilmelidir.
* Antivirüs: Sistem, bilgisayarı ve ağları virüslere, solucanlara, casus yazılımlara ve diğer kötü amaçlı yazılımlara karşı koruyabilmelidir.
* Gerçek Zamanlı Tarama: Sistem, dosyaları, e-postaları ve web trafiğini gerçek zamanlı olarak tarayabilmelidir.
* Tanıma ve Karantina: Sistem, virüsleri ve diğer kötü amaçlı yazılımları tanımlayabilmeli ve karantinaya alabilir veya silebilmelidir.
* Güncellemeler: Sistem, virüs tanımlarını ve diğer kötü amaçlı yazılım koruma güncellemelerini otomatik olarak indirebilmelidir.
* Spam Filtreleme: Sistem, spam e-postaları gelen kutusu ile spam klasörü arasında ayırt ederek gelen kutunuzu spamden korumalıdır.
* Spam Tanıma: Sistem, spam e-postaları spam filtreleme kurallarına göre otomatik olarak tanımlayabilmelidir.
* Kullanıcı Kontrolü: Kullanıcılara spam filtreleme kurallarını özelleştirme imkanı sağlanmalıdır.
* URL Filtreleme: Sistem, web sitelerine ve diğer çevrimiçi kaynaklara erişimi kontrol ederek uygunsuz içerikleri engelleyebilmelidir.
* URL Kara Listesi: Sistem, önceden tanımlanmış uygunsuz web sitelerini otomatik olarak engelleyebilmelidir.
* Web Kategorisi Filtreleme: Sistem, web sitelerini kategorilere göre sınıflandırabilmeli ve belirli kategorilere erişimi engelleyebilmelidir.

1. Performans Gereksinimleri

* Yüksek Erişilebilirlik: Sistemin kesintisiz çalışmasını sağlama. Yedekleme ve felaket kurtarma mekanizmalarının uygulanması.
* Ölçeklenebilirlik: Sistemin büyüyen ihtiyaçlara göre ölçeklendirilebilir olması. Artan trafik ve kullanıcı yüküne karşı dayanıklılık.
* Düşük Gecikme Süresi: Sistem, kullanıcıların ağa erişiminde ve web sitelerini ve diğer çevrimiçi kaynakları kullanırken gecikme yaşamamasını sağlayabilmelidir.
* Yüksek Yanıt Verme Hızı: Sistem, siber tehditlere ve diğer olaylara hızlı bir şekilde yanıt verebilmelidir.
* Yüksek Hacimli Trafik İşleme Kapasitesi: Sistem, yüksek hacimli ağ trafiğini işleyebilmelidir.
* 7/24 Kesintisiz Çalışma: Sistem, 7 gün 24 saat kesintisiz olarak çalışabilmelidir.

1. Güvenlik Gereksinimleri

* Veri Gizliliği ve Bütünlüğü: Tüm verilerin şifrelenmiş olarak saklanması ve iletilmesi. Veri bütünlüğünü koruyacak mekanizmaların uygulanması.
* Yetkilendirme ve Kimlik Doğrulama: Kullanıcıların yetkilendirilmiş erişimlerinin sağlanması. İki faktörlü kimlik doğrulama ve diğer güvenlik önlemleri.
* Güvenlik Güncellemeleri: Sistem, düzenli olarak güvenlik güncellemeleri ile güncellenmelidir.
* Güvenlik Olaylarına Yanıt Verme: Sistem, siber güvenlik olaylarına hızlı ve etkili bir şekilde yanıt verebilmelidir.
* Uyumluluk: Sistem, ilgili tüm yasalara, düzenlemelere ve sektör standartlarına uymalıdır.

1. Kullanılabilirlik Gereksinimleri

* Kullanıcı Eğitimi ve Destek: Kullanıcıların yeni sistemi hızlıca öğrenmesi için eğitim programları. Sürekli teknik destek ve yardım masası hizmetleri.
* Dokümantasyon: Sistem bileşenlerinin ve entegrasyon süreçlerinin detaylı dokümantasyonu. Kullanıcı kılavuzları ve teknik belgeler.
* Kolay Kullanım: Sistem, kullanımı kolay ve anlaşılır bir arayüze sahip olmalıdır.
* Çok Dilli Destek: Sistem, Türkçe ve İngilizce olmak üzere en az iki dilde destek sunmalıdır.

1. Entegrasyon Gereksinimleri

* API ve Protokoller: Farklı sistemlerin entegrasyonu için standart API ve protokollerin kullanımı. Veri ve olayların güvenli ve uyumlu şekilde paylaşılması.
* Uyumluluk Testleri: Entegrasyon süreçlerinde uyumluluk testlerinin gerçekleştirilmesi. Entegre sistemlerin performans ve güvenlik testlerinin yapılması.

1. İşlevsel Olmayan Gereksinimler

* Sistem, karmaşık ve kullanımı zor olmamalıdır.
* Sistem, pahalı olmamalıdır.
* Sistem, mevcut BT altyapısıyla uyumlu olmalıdır.

1. Ek Gereksinimler

* Sistem, yedekleme ve kurtarma işlevleri sağlayabilmelidir.
* Sistem, uzaktan erişim ve yönetim imkanı sağlayabilmelidir.