Bir Kurumsal Ağın ve Güvenlik Yapılarının Modellenmesi
Modeling and Analysis of an Enterprise Network and Its Security Structures

Deniz Akbaş[1], Halûk Gümüşkaya[2]

[1]Bilgisayar Mühendisliği Bölümü
Haliç Üniversitesi, Şişli, İstanbul
DenizAkbas@hsbc.com.tr

[2] Bilgisayar Mühendisliği Bölümü
Gediz Üniversitesi, Menemen, İzmir
haluk.gumuskaya@gediz.edu.tr

Özet

Bu makalede, tipik bir kurumsal ağın ağ cihazları ile gerçek ve OPNET yazılımı ile sanal modellenmesi, simülasyonu ve analizi yapılmıştır. Gerçek ve sanal kurumsal ağ modelleri üzerinde, Güvenlik Duvarı ve VPN'in (Sanal Özel Ağ) ağ performansına olan etkileri incelenmiştir. Daha sonra, kurumsal ağın ilk basit OPNET modelinin, daha karmaşık ve gerçekçi bir modeli oluşturulmuş ve bu model üzerinde benzer analiz çalışmaları yapılmıştır. Bu çalışmamızda daha önce yapılmış araştırma çalışmalardan farklı olarak, bir kurumsal ağın hem gerçek modeli hem de sanal simülasyon modeli oluşturularak, ağ modellerinin ve ağ trafik analiz sonuçlarının karşılaştırılması yapılmıştır. Güvenlik Duvarı ve VPN'in bu modellere olan etkilerinin araştırılması, hem gerçek ağ ortamında hem de sanal OPNET ortamında yapılmıştır. Ayrıca geliştirilen her iki gerçek ve sanal modelin üniversite eğitiminde pratik kullanımı da düşünülmüştür.

Abstract

In this paper, real modeling using network devices and virtual modeling with the OPNET software, simulation and analysis of a typical enterprise network are conducted. On these real and virtual network models, the effects of Firewall and VPN (Virtual Private Network) on network performance are studied. Then a more complex and realistic model than the first simple OPNET model is designed, and on this second model similar analysis work is performed. What we have done different than the previous research studies in our study is constructing both a real enterprise network prototype and virtual simulation model, and comparing network models and network analysis results. The effects of Firewall and VPN on these models are investigated on both real network environment and virtual OPNET environment. Additionally, practical use of both developed real and virtual models in university education is also taken into consideration.

1. Giriş

Kurumsal ağ (enterprise network), bir kurumun bölümlerini, yerel kullanıcılarını ve uzak kullanıcılarını birbirine bağlar, bilgi işlem ve iletişim kaynaklarına erişim sağlar. Genel olarak büyük yapılardan oluşur ve yapısında katı güvenlik kuralları ile çok sayıda uygulama bulundurur. Kurumsal ağlar yüzlerce kullanıcıyı destekleyebildiği gibi, geniş yapıda olanlarda bu sayı yüz binlere ulaşmaktadır.

Bir kurumsal ağ gerçekleştirilmeden önce, kurumsal ağın tasarımı aşamasında, güvenilir bir simülasyon aracı ile kurumsal ağ senaryoları oluşturarak, kurum ağının önce bir sanal ortamda tasarlanması, ağ uygulamalarının kulanım ve ağ trafik simülasyonlarının yapılması ve tasarımların doğrulanması, maliyet ve zaman tasarrufu sağlayacaktır.

Bu çalışma, bir kurumsal ağı ve bu ağdaki önemli güvenlik yapılarının gerçek ve sanal bir ortamda modellenmesini, simülasyonunu ve doğrulanmasını amaçlamaktadır. Bu çalışmanın diğer önemli bir amacı, günümüz kurumsal ağ donanım ve yazılım kavramlarını ve güvenlik yapılarını laboratuar çalışmalarıyla kısmen gerçek kısmen sanal ortamlarda öğrencilere öğretme yollarının araştırılmasıdır.

2. İlgili Çalışmalar

Ağ modellenmesi, simülasyonu ve doğrulanması konusunda birçok çalışma yapılmıştır [1], [2], [3], [4]. Bunlardan [1] ağ teknolojileri ve protokollerine yönelik araştırma ve eğitim çalışmaları için uygun simülasyon araçlarına bir giriş yapmaktadır. Bu çalışmada, ağ simülasyon araçlarının sahip olması gereken temel özellikler verilerek, bazı önemli simülasyon yazılımları sunulmaktadır. Simülasyon araçlarından gelişmiş bir ağ simülasyon aracı olan OPNET'in özellikleri ayrıntılı olarak verilmektedir. OPNET ile yapılan ağ modelleme araştırmalarından [2]'de, Poisson gibi geleneksel trafik modellerinin, gerçek ağ trafiğindeki ani artan davranışları açıklamada uygun olmadığı belirtilerek, bu modellere dayalı performans analizlerinde, paket gecikmesi ya da kaybolmalarının ciddi boyutlarda ihmal edebileceği vurgulanmaktadır. Bu çalışmada, Bernoulli kaynaklarının

hiyerarşik şeması üzerine kurulmuş yeni bir trafik modeli sunulmaktadır. Diğer araştırma çalışması [3], Ethernet ve Frame Relay ağ teknolojilerinden oluşan kurumsal ağ yapılarına yönelik karmaşık performans tahmini için, OPNET ile yapılan bir çözüm sunmaktadır. [4]'te, çeşitli bilgisayar ağı simülatörleri karşılaştırılmış ve OPNET ayrıntılı olarak tanıtılmıştır. OPNET ile ağ modeli gerçekleştirmedeki bazı ayrıntılar verilmiştir. Bu çalışmada ayrıca bazı simülasyon örnekleri de gösterilmiştir.

OPNET ile ağ güvenlik yapılarının modellenmesi üzerine de çeşitli çalışmalar yapılmıştır [5], [6]. Bunlardan [5]'de, ağ yöneticilerinin korkuları ya da önyargılarından dolayı ağ güvenliğinin, gerçek yaşamda etkinliğini ölçmenin zorluğuna değinerek, gerçek hayatta aşılması zor olan bu probleme OPNET simülasyon yöntemi ile bazı çözüm yolları sunulmuştur. [6]'da yaygın ağ güvenliği yapılarından olan Güvenlik Duvarı ve saldırı tespit sistemleri (IDS) sunulmaktadır. Bu çalışma OPNET ile kurumsal ağlarda kullanılabilir bir IDS uygulaması geliştirmeyi incelemektedir.

OPNET'in haberleşme ağları eğitiminde kullanım alanları ve şekilleri üzerine bir çok araştırma ve proje yapılmıştır [7], [8], [9], [10]. Bunlardan [7]'de, ağ teknolojisi derslerinde kullanılmak üzere OPNET IT Guru Akademik simülasyon ortamı ile geliştirilen laboratuar çalıştırmaları sunulmakta ve gerçek zamanlı ağlar ve protokoller için bu laboratuar sonuçları analiz edilmektedir. [8]'de, OPNET'in gelecekteki ağ mühendislerinin pratik becerilerini arttırarak gelişmiş ağ eğitimlerinde nasıl uygulanabileceği tartışılmaktadır. [9]'da, öğrencilerin kullandığı ağ uygulamalarının, Rowan Üniversitesi ağı üzerindeki etkileri incelenmektir. Bu çalışmada Rowan Üniversitesi'ndeki bir bilgisayar laboratuarının simülasyon modeli sunulmaktadır. Simülasyon OPNET Modeler ile gerçekleştirilmiş ve ağ paketleri Ethereal kullanılarak analiz edilmiştir. [10]'da başka bir üniversitedeki laboratuar çalışması ayrıntılı olarak sunulmaktadır. Yüksek lisans öğrencileri 2000-2001 akademik yılı süresince kiralık hatlar üzerinde ses trafiği, Ethernet üzerinde VoIP veya bir ofis LAN'ı üzerinde dosya paylaşımı çalışmalarından birini yapmışlardır. Her projede dört kısım bulunmaktadır: trafik yükü ölçümü, analitik performans hesaplamaları, simülasyonlar ve pratik bir laboratuar uygulaması. Simülasyonlar OPNET Modeler ile yapılmıştır.

Bizim çalışmamızda [11], yukarıda incelediğimiz daha önce yapılmış çalışmalardan farklı olarak, gerçek bir kurumsal ağ modeli ve OPNET sanal modeli oluşturularak, bu modeller üzerinde ağ ve güvenlik yapılarının analiz sonuçlarının karşılaştırılması yapılmıştır. Ayrıca, geliştirilen modellerin üniversite eğitiminde pratik kullanımı da düşünülmüştür.

3. Kurumsal Ağın Modellenmesi

Kurumsal ağ modellenmesi konusundaki çalışmamızda önce, günümüz kurumsal ağ yapıları incelenmiştir. Tipik ağ mimarileri ve kurumsal ağ modelleri, kurumsal ağlarda kullanılan yönlendirici ve anahtarlar gibi donanım cihazları, kurumsal ağ sunucuları, uygulamaları ve Güvenlik Duvarı, VPN gibi güvenlik yapıları araştırılmıştır.

Bu araştırmalarımız sonunda, ilk olarak örnek bir kurumsal ağ prototip modeli tasarlanmış, gerçek ağ cihazları ile gerçekleştirilmiş, değişik ağ trafiklerinin paketleri toplanarak analiz edilmiştir. Bu gerçek modelde Güvenlik Duvarı ve VPN'in ağ performansına olan etkileri incelenmiştir.

Daha sonra yapılan ikinci çalışmada, bu gerçek ağ prototipinin OPNET ortamında sanal bir modeli oluşturulup benzer testler yapılmıştır. OPNET ile yapılan çalışmada da Güvenlik Duvarı ve VPN'in ağ performansına olan etkileri incelenmiştir. Daha sonra gerçek ve sanal ortamda alınan analiz sonuçları karşılaştırılmıştır.

Üçüncü ve son çalışma olarak, daha karmaşık ve gerçekçi bir kurumsal ağ modeli OPNET'te tasarlanmış ve bu model üzerinde de benzer analiz çalışmaları yapılmıştır. Güvenlik yapılarının ağ performansına olan etkileri incelenmiştir.

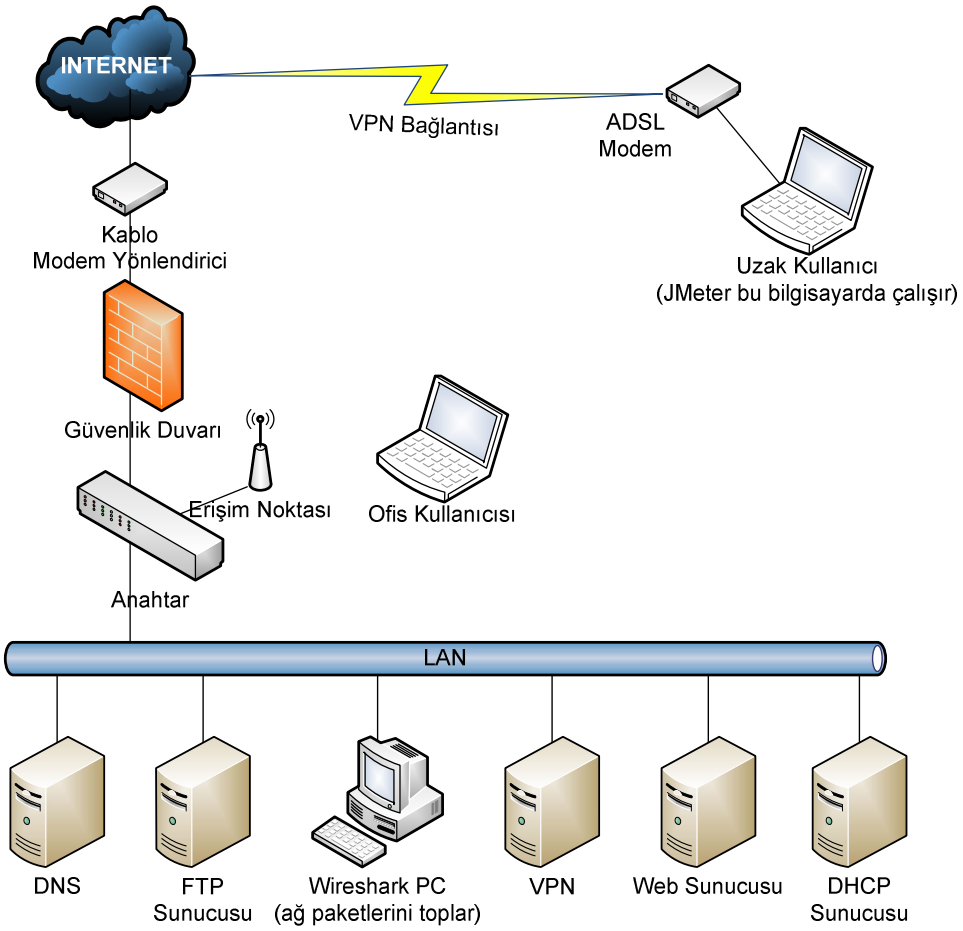
4. Gerçek Olarak Kurumsal Ağ Modellenmesi

Çalışmamızda gerçek kurumsal ağ modelinin tasarımında ve gerçekleştirilmesinde, Şekil 1'de görüldüğü gibi, en temel kurum ağı bileşenleri kullanılmıştır. Tasarlanan yapı iki farklı alandan oluşmaktadır. Birinci alan kurumsal ağ cihazlarının, sunucularının ve uygulamalarının yer aldığı iç kurum yerel ağıdır. İkinci alan ise bir dış bağlantı (örneğin ADSL) ile VPN bağlantısı üzerinden kurum ağına ulaşıldığı uzak bağlantının olduğu kısımdır. Kurum modeline uzaktan bağlantı için ADSL Modem, kurum modelinden Internet erişimi için NETMASTER CXC-150 Kablo Modem, Linux IPTables Güvenlik Duvarı, Linux OpenVPN Sanal Özel Ağ (VPN) Sunucusu, Microsoft DNS Server, Windows 2008-IIS 7.0 Web Sunucusu, Windows 2008- IIS 7.0 FTP Sunucusu, Linux DHCP Sunucusu ve Wireshark paket toplama aracının çalıştığı Windows XP kullanıcı PC'si yer almaktadır.

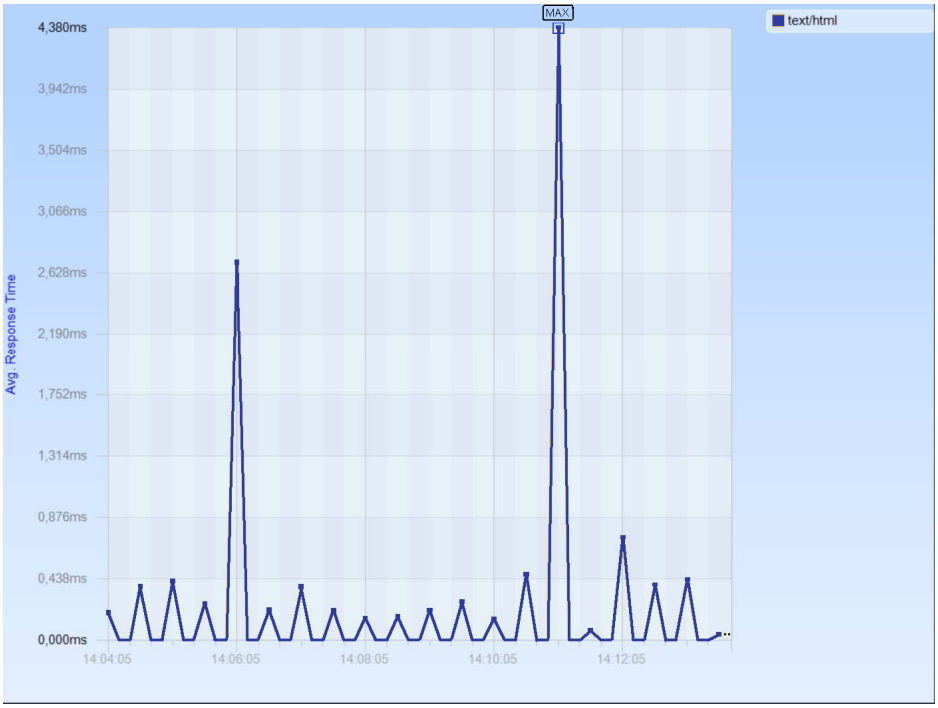
Güvenlik Duvarı, Internet ve yerel ağ trafiğinin denetlemesini yapan yazılımdır. Güvenlik Duvarı sayesinde Internet ve yerel ağ üzerinden belirli port'ların ya da belirli IP adreslerinin veya IP gruplarının erişimini engelleyebiliriz. Güvenlik Duvarı olarak kullanılan IPTables neredeyse tüm Linux sürümleri ile birlikte hazır gelmektedir. Kurumsal ağ yapımızda, IPTables en başarılı Linux sürümlerinden biri olan Open Suse 11 üzerinde çalışmaktadır.

Gerçekleştirilen kurumsal ağ modelinde, kurum dışında bulunan ve kurum kaynaklarına erişmek isteyen kullanıcılar için, yerel ağda bulunan bir sunucu üzerinde OpenVPN kurulumunu çalıştırarak, kullanıcılar için oluşturduğumuz sertifikaların kullanımı ile kurum ağına erişim sağlandı.

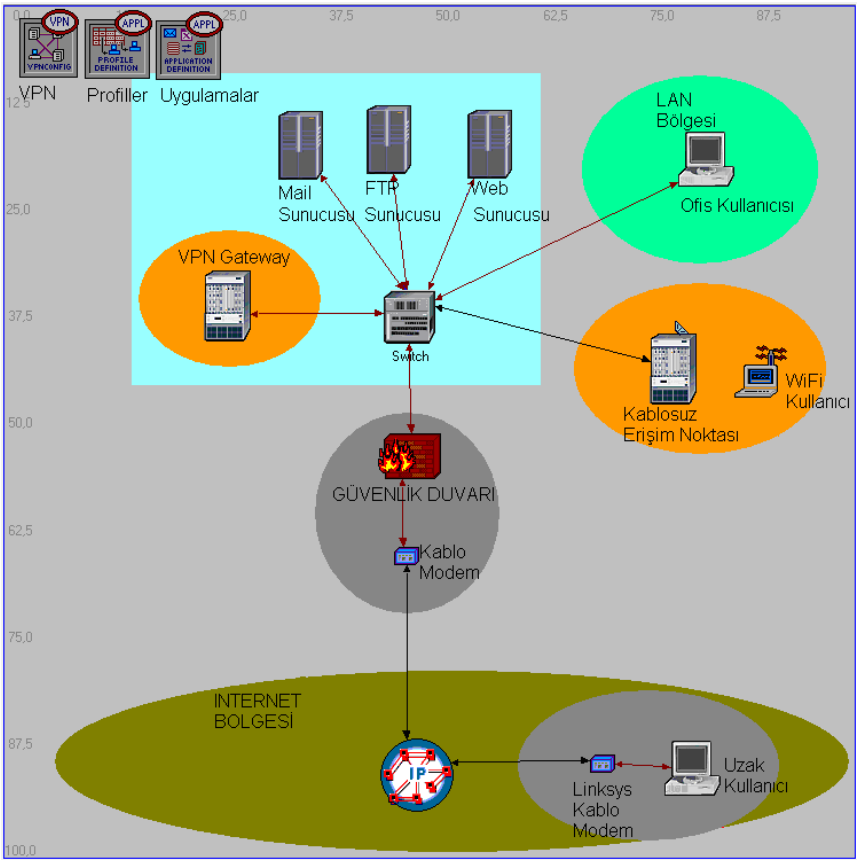
Test işlemleri, modelimizdeki kurum ağına Internet'te uzaktan erişim için kurulan VPN uzak bağlantısı üzerinden gerçekleştirildi. Bu bağlantı üzerinden JMeter [12] ile 30 sn aralılarla IIS 7.0 Web sunucusuna HTTP istekleri gönderilmiştir. Test süresi 10 dk olarak belirlenmiş olup, test sırasında Wireshark paket yakalama aracıyla ağ paketleri ve Windows Performans Monitor aracı ile de sunucu üzerindeki performans bilgileri toplanmıştır.



Şekil 1: Kurumsal ağ modeli.



Şekil 2: Web sunucusu istek-cevap süreleri.



Şekil 3: Gerçek kurumsal ağ modelinin OPNET ile oluşturulmuş modeli.

Windows Performans Monitor aracı, sunucular üzerinde çalışır ve birçok nesnenin değişik kriterlere göre analiz edilmesini sağlar. Örnek olarak "Web Service instance" nesnesinin altında bulunan web sitesi nesnesi, saniyede alınan, gönderilen ve toplam alınan-gönderilen veri miktarı gibi değişik sayaçlar vasıtası ile web servisinin çalışmasının ve performansının izlenebilmesini sağlar.

Wireshark ile toplanan ağ paketlerinin CACE Pilot [13] ile değişik analiz sonuçları alınmıştır. Bu program ile elde edilen test sonuçlarından web sunucusu istek-cevap sürelerine ait bir grafik Şekil 2'de verilmektedir. CACE Pilot, Wireshark'ın kullanımına bir boyut katan, Wireshark ile toplanan kablolu ve kablosuz ağ paketleri için, görsel açıdan zengin ve güçlü analiz yetenekleri sağlayan bir ağ analiz aracıdır. CACE Pilot'tan alınan veriler ile OPNET ortamından alınan verilerin karşılaştırılması yapılmıştır. Şekildeki maksimum değerler, Internet yoğunluğuna bağlı olarak değişiklik göstermiştir.

5. OPNET ile Kurumsal Ağ Modellenmesi

Gerçek ağ cihazları ile gerçekleştirilen kurumsal ağ modelinin, daha sonra Şekil 3'te görülen OPNET ortamındaki sanal bir modeli oluşturuldu. Oluşturduğumuz senaryonun gerçek ortamla aynı olması için, yapımızda 2 adet xDSL Modem, 3 adet ethernet_server, bir adet ethernet_16_switch, 2 adet ethernet_workstation, 1 adet vlan_ethernet_router, 1 adet wlan_wkstn, dışarıdan VPN erişimi sağlamak için 1 adet ethernet_4_slip_gtwy ve bileşenler arası bağlantıyı sağlamak için 10Base_T_LAN ve PPP internet bağlantı linkleri kullanılmıştır.

OPNET modelindeki uygulamalar ve bu uygulamaların hangi kullanıcılar tarafından kullanılacağının tanımını yapmak için 'Application Config' ve 'Profile Config' bileşenleri eklenmiştir. VPN ayarları 'VPN Config' nesnesi ile yapılmaktadır. Bu aşamadan sonra, sistemdeki uygulamalar tanımlanmış ve hangi bileşenlerin hangi uygulamalar için kullanılacağı belirlenmiştir.

Yapılan ayarlardan sonra, bu model üzerinde daha önceki gerçek ağdakine benzer senaryolar oluşturularak ağ trafiğinin değişik grafikleri elde edildi. OPNET sanal ortamında alınan sonuçların gerçek ortamda elde edilen sonuçlara çok yakın olduğu gözlendi.

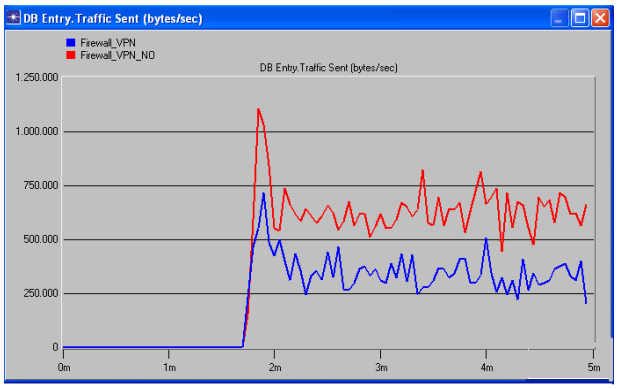
Çalışmamızda daha gerçekçi bir kurum ağı tasarımı için OPNET'teki model geliştirildi. Yeni modeldeki kurumun yapısı, İstanbul Genel Müdürlük, İzmir Bölge ve Ankara Bölge olmak üzere üç farklı noktadan oluşmakta olup 385 tane çalışanı vardır. İzmir ve Ankara İnternet erişimlerini genel müdürlük üzerinden sağlamaktadır.

Yeni modelimizde, dış bölge diye nitelendirdiğimiz alanda Web Sunucusu ve Dosya Aktarım (FTP) Sunucusu, yerel sunucu bölgesi olarak tanımladığımız alanda da Posta Sunucusu, Veritabanı Sunucusu ve Dosya Sunucusu olmak üzere toplam beş sunucu bulunmaktadır. Bu kurumda, 'Engineer', 'Researcher', 'E-Commerce Customer', 'Sales Person', 'Multimedia User', 'Hacker Group' adlı

kullanıcıların bulunduğu kurum içi ve dışından gelen trafik incelenmiştir.

Daha gerçekçi olan bu model üzerinde Güvenlik Duvarı ve VPN kullanımının sisteme olan etkileri iki farklı senaryo ile incelendi. Birinci senaryoda bu güvenlik yapıları bulunmamaktadır. İkinci senaryoda Güvenlik Duvarı ve VPN kullanılmakta olup bu yapıların ve yetkisiz erişimlerin modelimizdeki beş sunucuya olan etkileri analiz edilmiştir.

Güvenlik Duvarı ve VPN güvenlik yapılarının, yetkisiz erişimleri engellemesinin yanında ağ trafiğini yaklaşık %20 oranında yavaşlattığı görülmüştür. Şekil 4'te Veritabanı ağ trafiğinin güvenlik yapıları kullanılarak ve bunlar olmadan elde edilen grafikler görülmektedir.



Şekil 4: Güvenlik Duvarı ve VPN'in ağ trafiğine olan etkisi.

6. Sonuçlar

Bu çalışmada önce bir temel kurumsal ağın gerçek ortamı oluşturuldu ve üzerinde ağ paket ölçümleri ve analizleri yapıldı. Bir VPN bağlantısı üzerinden kurum kaynaklarına erişim gerçekleştirildi. Oluşturulan kurum ağı içerisinde bulunan Web Sunucusuna, kurum ağı dışından Internet ortamında bulunan bir bilgisayardan Apache JMeter uygulaması ile istekler gönderildi. Gönderilen isteklerin Web Sunucusu ve ağ üzerindeki etkisini analiz etmek için, iç ağdaki bir bilgisayarda Wireshark ile ağ paketleri toplanarak CACA Pilot uygulaması ile toplanan verilerin grafikleri oluşturuldu. Analizler sonucunda Web Sunucusunun isteklere cevap süreleri ve ağ trafik değerleri, bize karşılaştırma yapabilmemiz açısından bir ölçüm aracı olmuştur.

İkinci olarak gerçek ağ modelinin benzeri OPNET ortamında gerçekleştirildi ve üzerinde simülasyonlar yapıldı. OPNET'teki modelde VPN bağlantısı ile Internet ortamından kurum ağı içinde bulunan Web Sunucusuna gönderilen isteklerin analizi yapılmıştır. Elde edilen simülasyon testleri sonucunun, gerçek ortam test sonuçlarına çok benzerlik gösterdiği ve OPNET simülasyon aracı ile yapılacak çalışma sonuçlarının gerçeğe oldukça yakın sonuçlar ürettiği gözlenmiştir.

Çalışmamızda üçüncü olarak sadece OPNET ortamında daha gerçekçi bir kurumsal ağ modeli geliştirilmiştir. Günümüzdeki önemli güvenlik yapıları dikkate alınarak, şehirlerarası bağlantıları olan bir kurumun da kullanabileceği ve faaliyetlerini güvenle gerçekleştirebileceği, dağıtık yapıda bir kurum ağı tasarlandı. Daha sonra bu model üzerinde çeşitli testler yapılarak güvenlik yapılarının ağ performansına olan etkileri incelenmiştir. Güvenlik Duvarı ve VPN kullanarak ve bu yapılar içermeyen iki farklı senaryo oluşturuldu. Bu iki senaryonun OPNET simülasyon test sonuçları incelenerek, Güvenlik Duvarı ve VPN'in kurum güvenliği ve ağ performansına olan etkileri analiz edildi.

Bu çalışmamızda sonuç olarak, bir kurumsal ağ gerçekleştirilmeden önce, kurumsal ağın tasarımı aşamasında, OPNET gibi güvenilir bir simülasyon aracı ile kurumsal ağ senaryoları oluşturarak, kurum ağının önce bir sanal ortamda tasarlanmasının, simülasyonlarının yapılmasının ve tasarımlarının doğrulanmasının, maliyet ve zaman tasarrufu sağlayacağı görülmüştür.

7. Kaynaklar

[1] Mohorko, J., Matjaz, F., Sasa, K., "Advanced Modelling and Simulation Methods for Communication Networks", *Microwave Review*, pp. 41-46, September, 2008.

[2] Potemans, J., Van den Broeck, B., Guan, Y., Theunis, J., Lil, E. Van, Capelle, A. Van de, "Implementation of an Advanced Traffic Model in OPNET Modeler", *OPNETWORK 2003*, 2003, Washington D.C., USA.

[3] Felten, J., Gurbuz , O., Owen, H., GroBmann, T., Kussmann, G., Schrock, W., "Modeling, Simulation, and Verification of an Enterprise Network", *Globol Telecommunications Conference – Globecom'99*, 1999.

[4] Chang, X., "Network Simulations with OPNET", *Proceedings of the 1999 Winter Simulation Conference*, 1999.

[5] Zaballos, A., Corral, G., Serra, I., Abella, J., "Testing Network Security using OPNET", *OPNETWORK'2003*, 2003, Washington DC, USA.

[6] G. Corral, A. Zaballos, J. Abella, C. Morales, "Building an IDS using OPNET", *OPNETWORK'2005*, 2005, Washington DC, USA.

[7] Kumar, A., "Development of Laboratory Exercıses Based on the Opnet Network Simulating Approach", *Rivier College Online Academic Journal*, Vol. 1, No. 1, 2005.

[8] Theunis, J., Van den Broeck, B., Leys, P., Potemans, J., Lil, E. Van, Capelle, A. Van de, "OPNET in Advanced Networking Education", *OPNETWORK 2002*, 2002, Washington D.C., USA.

[9] Hnatyshin, V., Lobo,A. F., Bashkirtsev, P., DeDomenico, R., Fabian , A., Gramatges, G., Metting, J., Simmons, M., Stiefel, M., "Modeling a University Computer Laboratory using OPNET Software", Computer Science Department, Rowan University, New Jersey, United States, 2006.

[10] Potemans, J., Theunis, J., Teughels, Lil, M., E. Van, Capelle, A. Van de, "Student Network Design Projects using OPNET", OPNETWORK 2001, 2001, Washington D.C., USA.

[11] Akbaş, D., *Bir Kurumsal Ağın ve Güvenlik Yapılarının Modellenmesi ve Analizi*, Haliç Üniversitesi, Bilgisayar Mühendisliği Bölümü-Yönetim Bilişim Sistemleri Programı, Yüksel Lisans Tezi, Temmuz 2010.

[12] JMeter: http://jakarta.apache.org/jmeter/ .

[13] CACE Pilot: www.cacetech.com .