T.C.
HALİÇ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ PROGRAMI

BİR KURUMSAL AĞIN VE GÜVENLİK YAPILARININ MODELLENMESİ VE ANALİZİ

YÜKSEK LİSANS TEZİ

Hazırlayan
Deniz AKBAŞ

Danışmanı
Prof. Dr. Halûk GÜMÜŞKAYA

İstanbul – Temmuz 2010

T.C.

HALİÇ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bilgisayar Mühendisliği Anabilim Dalı Yönetim Bilişim Sistemleri Programı Tezli Yüksek Lisans öğrencisi **Deniz AKBAŞ** tarafından hazırlanan **"Bir Kurumsal Ağın ve Güvenlik Yapılarının Modellenmezi ve Analizi"** adlı bu çalışma jürimizce Yüksek Lisans Tezi olarak kabul edilmiştir.

Sınav Tarihi : 21.07.2010

(Jüri Üyesinin Ünvanı , Adı , Soyadı ve Kurumu) : İmzası :

Jüri Üyesi: Prof.Dr.Haluk GÜMÜŞKAYA .....
Danışman–HAL.Üniv.Bilgisayar Müh. ABD Öğr.Üyesi

Jüri Üyesi : Yrd.Doç.Dr.Yüksel BAL .....
HAL.Üniv. Bilgisayar Müh. ABD Öğr.Üyesi

Jüri Üyesi : Yrd.Doç.Dr.Taha İMECİ .....
HAL.Üniv.Elek.ve Hab. Müh.ABD Öğr.Üyesi

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR LİSTESİ

ACK : ACKnowledgement
ACL : Access Control List
ADSL :Asymmetric Digital Subscriber Line
ARP : Address Resolution Protocol
ATM : Asynchronous Transfer Mode
BES : Back End Server
CPU : Central Processing Unit
DB : Database
DHCP :Dynamic Host Configuration Protocol
DNS : Domain Name System
DoS : Denial of Service
EIGRP : Enhanced Interior Gateway Routing Protocol
FTP : File Transfer Protocol
HIPS : Host Intrusion Prevention System
HTML : Hyper Text Markup Language
HTTP : Hypertext Transfer Protocol
HTTPS : Hypertext Transfer Protocol Secure
IDS : Intrusion Detection System
IGRP : Interior Gateway Routing Protocol
IIS : Internet Information Services
IP : Internet Protocol
IPS : Intrusion Prevention Systems
IPSEC : Internet Protocol Security
ISDN : Integrated Services Digital Network
ISP : Internet Service Providers
ITU : International Telecommunication Union
JBDC : Java Database Connectivity
L2TP : Layer 2 Tunnelling Protocol
LAN : Local Area Network
MAC : Media Access Control
MAN : Metropolitan Area Network
NAT : Network Address Translation
NMAP : Network Mapper
OPNET : OPtimized Network Engineering Tool
P2P : Peer to Peer
PPP : Point-to-Point Protocol
PPTP : Point to Point Tunnelling Protocol
PSTN : Public Switched Telephone Network
QoS : Quality of Servise
RIP : Routing Information Protocol
RTS : Request To Send
SIP : Session Initiation Protokol

Sn : Saniye
SSL : Secure Socket Layer
TCP : Transmission Control Protocol
URL : Uniform Resource Locator
VLAN : Virtual Local Area Network
VoIP : Voice Over Internet Protocol
VPN : Virtual Private Network
WAN : Wide Area Network
WPA : Wi-Fi Protected Access

GENEL BİLGİLER

Adı ve Soyadı : Deniz AKBAŞ
Anabilim Dalı : Yönetim Bilişim Sistemleri
Programı : Bilgisayar Mühendisliği
Tez Danışmanı : Prof. Dr. Halûk GÜMÜŞKAYA
Tez Türü ve Tarihi : Yüksek Lisans – Temmuz 2010

BİR KURUMSAL AĞIN VE GÜVENLİK YAPILARININ MODELLENMESİ VE ANALİZİ

ÖZET

Bu tezde, tipik bir kurumsal ağın önce bir prototip tasarım ile gerçek ve sonra OPNET yazılımı ile sanal olarak modellenmesi, simülasyonu ve analizi yapılmıştır. Gerçek ve sanal kurumsal ağ modelleri üzerinde, Güvenlik Duvarı ve VPN'in ağ performansına olan etkileri incelenmiştir. Daha sonra basit olan kurumsal ağın ilk OPNET modelinin, daha karmaşık ve gerçekçi bir modeli oluşturulmuş ve bu model üzerinde benzer analiz çalışmaları yapılmıştır. Bu tezde diğer bir araştırma konumuz OPNET'in haberleşme ağları eğitiminde kullanım alanları ve şekilleri olmuştur.

Tezde önce, günümüz kurumsal ağ yapıları genel olarak incelenmiştir. Tipik ağ mimarileri ve kurumsal ağ modelleri, kurumsal ağlarda kullanılan yönlendirici ve anahtarlar gibi donanım cihazları, kurumsal ağ sunucuları ve Güvenlik Duvarı, VPN gibi güvenlik yapıları sunulmuştur.

Tezin ana çalışmalarından ilki 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.

Tezde yapılan ikinci çalışma, bu gerçek ağ prototipinin OPNET ortamında sanal bir modelinin oluşturulması ve benzer testlerin yapılmasıdır. 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.

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

Bu tez çalışmasında daha önce yapılmış araştırma çalışmalardan farklı olarak, hem gerçek bir kurumsal ağ prototip modeli hem de sanal simülasyon modeli oluşturularak ağ modellerinin ve ağ trafik analiz sonuçlarının karşılaştırılması yapılmıştır. Bu modellere Güvenlik Duvarı ve VPN'in etkilerinin araştırılması, hem gerçek ortamda hem de sanal OPNET ortamında yapılmıştır. Ayrıca geliştirilen her iki gerçek ve sanal modelin üniversite eğitiminde pratik kullanımı da düşünülmüştür.

Anahtar Kelimeler: Kurumsal Ağ Modellenmesi ve Simülasyonu, OPNET, Güvenlik Duvarı, VPN

GENERAL INFORMATION

Name and Surname : Deniz AKBAŞ
Field : Management Information Systems
Program : Computer Engineering
Supervisor : Prof. Dr. Halûk GÜMÜŞKAYA
Degree and Date : Master – July 2010

MODELLING AND ANALYSIS OF AN ENTERPRISE NETWORK AND ITS SECURITY STRUCTURES

ABSTRACT

In this thesis, first, a prototype design as real modeling and using the OPNET software virtual modeling of a typical enterprise network are constructed, then simulated and analyzed. 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. In this thesis, another research topic is to investigate application areas and uses of OPNET in communication networks education.

In this thesis, first, current enterprise network structures are investigated in general. Typical network architectures and enterprise network models, hardware devices such as routers and switches used in enterprise networks, enterprise network servers and security structures such as Firewall and VPN are presented.

As the first of the thesis's main studies, a prototype model of an enterprise network is designed, implemented using real network devices, packets of various network traffics are captured and analyzed. The effects of Firewall and VPN on network performance are studied in this real model.

As the second work in this thesis, a virtual model of the real network prototype in the OPNET environment is constructed and similar tests are performed. The effects of Firewall and VPN on network performance are also studied in the OPNET model. Then the analysis results obtained in the real and virtual environments are compared.

As the third and last work in this thesis, a complex and realistic enterprise network model is designed in OPNET, and analysis work is performed on this model. The effects of security structures on network performance are investigated.

What we have done different than the previous research studies in this thesis 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 studied in both real and virtual OPNET environments. Additionally, practical use of both developed real and virtual models in university education is also taken into consideration.

Key Words: Enterprise Network Modeling and Simulation, OPNET, Firewall, VPN

1. GİRİŞ

Kurumsal ağ (enterprise network), bir kurumun faaliyetleri ile üretilen veya kurumun dış dünya ile yaptığı çalışmalar sonucu elde ettiği her türlü bilginin bir yerden bir yere iletilip kullanıcıların hizmetine sunulmasını sağlayan kablolar ve ağ cihazlarını kapsayan karmaşık bir yapıdır. Kurumsal ağlarının kullanımı sayesinde kurumlar kaynak ve zaman tasarrufu sağlamaktadır. Kurum çalışanları, dosya sunucuları üzerinden birbirlerinin verilerine erişebilir, program veya donanım paylaşımında bulunabilmektedir. Ağda bulunan ve paylaşıma açılmış bir çevre birimi (yazıcı, tarayıcı, DVD-ROM, modemler gibi) ağdaki tüm bilgisayarlar tarafından kullanılabilmektedir. Kaynakların paylaşımı aynı zamanda maliyet kazancı sağlamaktadır.

Bir kurumun ağ yapısında yer alan güvelik duvarları, saldırı tespit cihazları, VPN çözümleri ve anahtarlar üzerindeki VLAN ayarları, kurum güvenliğini sağlanması için kullanılan sistemler ve ayarlardır. Dış kullanıcının iletişimde kalabilmesi için VPN çözümleri ile, Internet üzerinden kurum ağına erişebilmesi gerekir. Tüm bu değişkenlerdeki hatalar sistemin güvenliğini tehdit eden unsurlardır.

1.1. Tezin Amacı

Bu tezin amacı, bir kurumsal ağı ve bu ağdaki önemli güvenlik bileşenlerinin gerçek ve sanal bir ortamda modellenmesi, simülasyonu ve doğrulanmasını amaçlamaktadır. Bu tez çalışmasının diğer önemli bir amacı, günümüz kurumsal ağ donanım ve yazılım kavramlarını ve güvenlik yapılarını laboratuar ortamlarında kısmen gerçek kısmen sanal ortamlarda öğrencilere öğretme yollarının araştırılmasıdır.

1.2. Tezin Yapısı

Bu tez sekiz bölümden oluşmaktadır. İlk bölümde giriş yapıldıktan sonra, ikinci bölümde, ilgili çalışmalar incelenerek özetlenmiştir. Üçüncü bölümde kurumsal ağ yapıları genel olarak incelenmiş, genel ağ mimarileri ve kurumsal ağ modelleri, kurumsal ağ yapılarında kullanılan yönlendirici ve anahtarlar gibi donanım cihazları, kurumsal ağ sunucuları ve kurumsal ağlarda kullanılan Güvenlik Duvarı (Firewall), VPN gibi güvenlik yapıları sunulmuş, ağ benzetim araçları anlatılmıştır. Tezde kullanılan OPNET benzetim aracının özellikleri hakkında bilgiler verilmiştir.

Dördüncü bölümde, bir kurumsal ağ modeli için tez çalışmasında geliştirilen gerçek ve simülasyon ortamları ayrıntılı olarak anlatılmış, yapılan testler sunulmuş ve elde edilen sonuçlar karşılaştırılmıştır. Beşinci bölümde günümüz teknolojileri düşünülerek örnek bir kurum ağı tasarlanarak kurumun Internet erişimi, VPN alt yapısı anlatılmıştır.

Altıncı bölümde, beşinci bölümde tasarımı sunulan kurumsal ağ yapısına, Güvenlik Duvarı ve VPN güvenlik yapılarının eklenmesiyle OPNET benzetim programının gerçekleştirebildiği yapı çerçevesinde benzetimi yapılarak, bu yapıların ağ performansına etkileri karşılaştırılmakta, sonuçlar analiz edilerek tez çalışmasının temelini oluşturan Kurumsal Ağların Güvenliği ile ilgili karşılaştırmalı bir inceleme yapılmıştır.

Yedinci bölümde tez çalışmasında elde edilen sonuçlar özetlenmekte ve sekizinci bölümde tezin akademik ve diğer kaynakları verilmektedir.

2. İLGİLİ ÇALIŞMALAR

2.1. Giriş

Bu bölümde, tez çalışmalarımıza kaynak oluşturan önemli akademik çalışmalar incelenmiş ve bu çalışmaların katkıları özetlenmiştir. Özellikle tezimizin ana konusu çerçevesinde kurumsal ağ yapılarının bir prototip tasarım ile gerçek ve OPNET yazılımı ile sanal olarak modellenmesi, simülasyonu ve analizi üzerine yapılan çalışmalar araştırılmıştır. Ayrıca kurumsal ağlardaki önemli güvenlik ağ yapılarının modellenmesi de diğer ikinci bir araştırma konumuz olmuştur. Üçüncü araştırma konumuz OPNET'in haberleşme ağları eğitiminde kullanım alanları ve şekilleri olmuştur.

2.2. Akademik Çalışmalar

OPNET yazılımı kullanılarak yapılan ağ modellenmesi, simülasyonu ve doğrulanması konusunda birçok çalışma yapılmıştır [1], [2], [3], [4]. Bunlardan [1] ağ teknolojileri ve protokollerine yönelik araştırma ve eğitim için uygun simülasyon araçlarına güzel bir giriş yapmaktadır. Bu çalışmada ağ simülasyon araçlarının sahip olması gereken temel özellikleri verilerek, bazı önemli simülasyon yazılımları sunulmaktadır. Bu simülasyon araçlarından gelişmiş bir ağ simülasyon aracı olan OPNET'in özellikleri ayrıntılı olarak verilmektedir. Ağ simülasyon araçları arasında yaygın kullanılan bu aracının, hem ağ simülasyonları için, hem eğitimler için, hem de yeni Internet cihazları ve protokolleri araştırmaları için uygun olduğu belirtilmektedir. OPNET'in temel paketinin, iletişim ağlarının simülasyonu, protokolleri ve cihazları geliştirmek için tasarlandığı belirtilmekte, bunun yanında diğer gelişmiş özelliklerinin de olduğu sunulmaktadır. OPNET'in, kablosuz ağların simülasyonu için ACE modülü, sanal arazide ağlar görüntülenmesi için 3DNV modülü ve gerçek zamanlı çevrim içindeki gerçek haberleşme cihazlarının bulunduğu ağ simülasyonları için bir modülünün (system in the loop) olduğu belirtilmektedir.

OPNET ile yapılan ağ modelleme araştırmalarından [2]'de, Poisson gibi geleneksel trafik modellerinin, gerçek ağ trafiğindeki ani artan davranışlarını açıklamada uygun doğru model olmadığı belirtilerek, bu modellere dayalı performans analizlerinin, 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]'de, Ethernet ve Frame Relay ağ teknolojilerinden oluşan kurumsal ağ yapılarına yönelik karmaşık performans tahminine için, OPNET kullanarak yapılan bir çözüm sunmaktadır. [4]'de, birçok bilgisayar ağı simülatörleri karşılaştırılmış, OPNET ayrıntılı olarak tanıtılmıştır. OPNET üzerinde ağ modellerinin gerçekleştirilme ayrıntıları verilmiştir. Bu çalışmada bazı simülasyon örnekleri de gösterilmiştir.

OPNET ile ağ güvenlik yapılarının modellenmesi üzerine de çeşitli çalışmalar yapılmıştır [5] ve [6]. Çalışma [5]'de, ağ yöneticilerinin korkuları ya da önyargılarından dolayı ağ güvenliğinin, gerçek yaşamda etkinliğini ölçmenin zorluğuna değinerek, gerçek hayatta aşılması zor olan bu problemlere bir çözüm bulmak amacıyla OPNET simülasyon yöntemi ile bazı çözüm yolları sunulmuştur. [6]'da en yaygın ağ güvenliği bileşenlerinden 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 incelemektir. Bu çalışmada Rowan Üniversitesi'ndeki bir bilgisayar laboratuarının simülasyon modeli sunulmaktadır. Simülasyon OPNET Modeller yazılım paketi kullanılarak gerçekleştirilmiş ve ağ paketleri Ethereal (Wireshark) kullanılarak analiz edilmiştir. [10]'da 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 çalışmasından birini yapmışlardır. Her projede dört kısım bulunmaktadır: trafik yükü ölçümü, analitik performans hesaplamaları, simülasyonlar ve pratik bir laboratuar uygulaması. Simülasyonlar OPNET Modeller ile yapılmıştır.

Bizim tez çalışmamızda, yukarıda incelediğimiz, daha önce yapılmış çalışmalardan farklı olarak, gerçek bir kurumsal ağ prototip ortamı ile simülasyon ortamları oluşturularak sonuçları karşılaştırılmasıdır. Ayrıca geliştirilen her iki gerçek ve sanal modelin üniversite eğitiminde pratik kullanımı da düşünülmüştür.

3. İLGİLİ KONULAR

3.1. Kurumsal Ağ Yapıları

Kurumsal ağın amacı kurumun iş hedefleri doğrultusunda çok farklı ağ uygulamasını desteklemesidir. Kurumsal ağ, kurumun alt bölümlerini, yerel kullanıcıları ve uzak kullanıcılarını birbirine bağlar, bilgi işlem ve iletişim kaynaklarına ara bağlantı ile ulaşarak kurum çapında yarar oluşturmasını sağlar. Genel olarak büyük yapılardan oluşurlar ve yapılarında katı güvenlik kuralları içerisinde çok sayıda uygulama bulundururlar. Kurumsal ağlar yüzlerce kullanıcıyı destekleyebildiği gibi, geniş yapıda olanlarda bu sayı yüz binlere ulaşmaktadır.

Kurumsal ağlar bilgisayarlar, yazıcılar ve sunucular gibi pek çok sistemi birbirine bağlayarak veri alışverişini sağlar. Kurumsal ağlar ile veri paylaşımı, elektronik-posta kullanımı, çevre birimlerinin paylaşımı ve uygulamaların ortak kullanımı sağlanır. Kurumsal ağlarının bir diğer kullanım alanı ise yazıcılar gibi çevre birimlerinin paylaşımı ile kaynak kullanımını yönetmektir. Kurumsal ağ ortamlarında, bilgilerin birimler ve şubeler arasında paylaşılması, elektronik posta gönderimi, belgeleri birlikte oluşturmak gibi olanaklar kullanıcılara ve kurumlara büyük faydalar sağlar.

Bilgisayar sistemleri kullanımının zaman içerisinde artmasıyla sistemlerin yönetimini ve güvenliğinin daha iyi sağlanabilmesi için Bilgi İşlem Merkezleri oluşturulmaktadır. Sunucular (server), ana bilgisayarlar (main frame), güvenlik duvarları, ağ cihazları, ağ bağlantıları ve saldırı tespit sistemleri Bilgi İşlem Merkezilerini oluşturan en önemli parçalardır.

Bir ağ yapısı içerisinde bilgisayar sistemlerinin ve ortamın tasarımı, ağ mimarisi olarak isimlendirilebilir ve günümüzde en yaygın olarak istemci/sunucu ve peer-to-peer olarak gruplandırılır.

Peer-to-Peer mimarisinde, ağ içerisindeki bilgisayarlar herhangi bir sunucuya ihtiyaç duyulmadan birbirleri ile doğrudan iletişim kurarlar. Az sayıda bilgisayarı bağlayan basit ve ucuz bir ağ modelidir. Her bilgisayarda ağdaki diğer bilgisayarların adresleri bulunur ve bilgisayarlar bu adreslerden, hizmet almak istediği bilgisayarı bulup erişim sağlayarak, işlemi gerçekleştirir. Sistemin yönetimi oldukça zordur ve sistemdeki işlemlerin takip edilmesi, kimin ne yaptığının takip edilmesi, imkansız denecek kadar zordur.

İstemci/Sunucu mimarisinde ise, ağdaki bazı bilgisayarlar sunucu olarak çalışırlar ve ağdaki diğer bilgisayarlar bu sunuculardan hizmet isteğinde bulunurlar. Dosya sunucusu; dosyaların

tutulması ve yönetimi için, baskı sunucusu; yazma görevleri için veritabanı sunucusu ise; verilerin depolanması ve bu verilere erişimin denetimi için kullanılır.

Bir kurumun, bir bölümü içerisinde; bir veya birkaç birim arasında ağ kartları, kablo ve anahtarlar gibi ağ cihazları ile oluşturulan ağ sistemine Yerel Alan Ağı (Local Area Network - LAN) denir. Yerel ağların temel amacı aynı bölge içinde kullanılan bilgisayarların çevre birimlerini ve kaynakları paylaşmasını, ortak çalışma imkanı oluşturarak bilginin hızlı bir şekilde işlenmesini sağlamaktır.

Bir yerleşke veya geniş bir bölge içerisinde, yönlendiriciler gibi ağ aygıtları yardımıyla, bünyesinde birden çok yerel ağ içeren ve birbirine bağlayan ağ sistemlerine de Orta Ölçekli Ağ (Metropoliten Area Network – MAN) İntranet sistemleri örnek verilebilir.

Geniş Alan Ağı (Wide Area Network – WAN) ise birden fazla orta ölçekli ağı birbirine bağlayan veya doğrudan dışarıdan modemler yardımıyla bağlanılarak, ağa erişim sağlanılabilen sistemlerdir. Sistem üzerinde on binlerce kullanıcı çalışabilir. Kullanıcı sayısı arttıkça hız düşer. Geniş alan ağına örnek olarak Internet verilebilir.

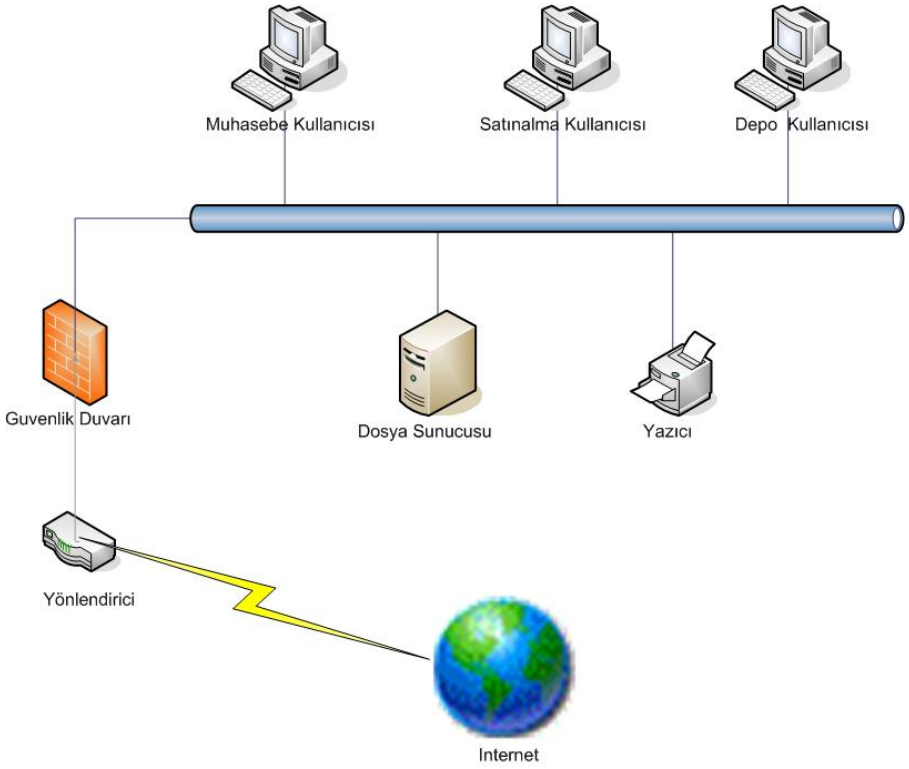
Ağ cihazları uç sistem durumunda olan sistemlerin, iletişim yapmalarını sağlayan cihazlardır. Kurumsal ağlar incelendiğinde ağ yapılarını oluşturan yazılımsal ve donanımsal birçok sistemin kullanıldığı gözlemlenmektedir.

Kurumsal ağlar; kurumların yapıları, büyüklükleri, ekonomik durumları ve ihtiyaçlarına göre oluşturdukları birçok ağ modeli ile karşımıza çıkmaktadırlar. Kurum ağ yapıları dünyanın çeşitli bölgelerinde olabileceği gibi, tek bir noktadaki yerel alan ağından da oluşabilir.

3.2. Ağ Mimarleri

3.2.1. Temel Kurumsal Ağ Yapısı

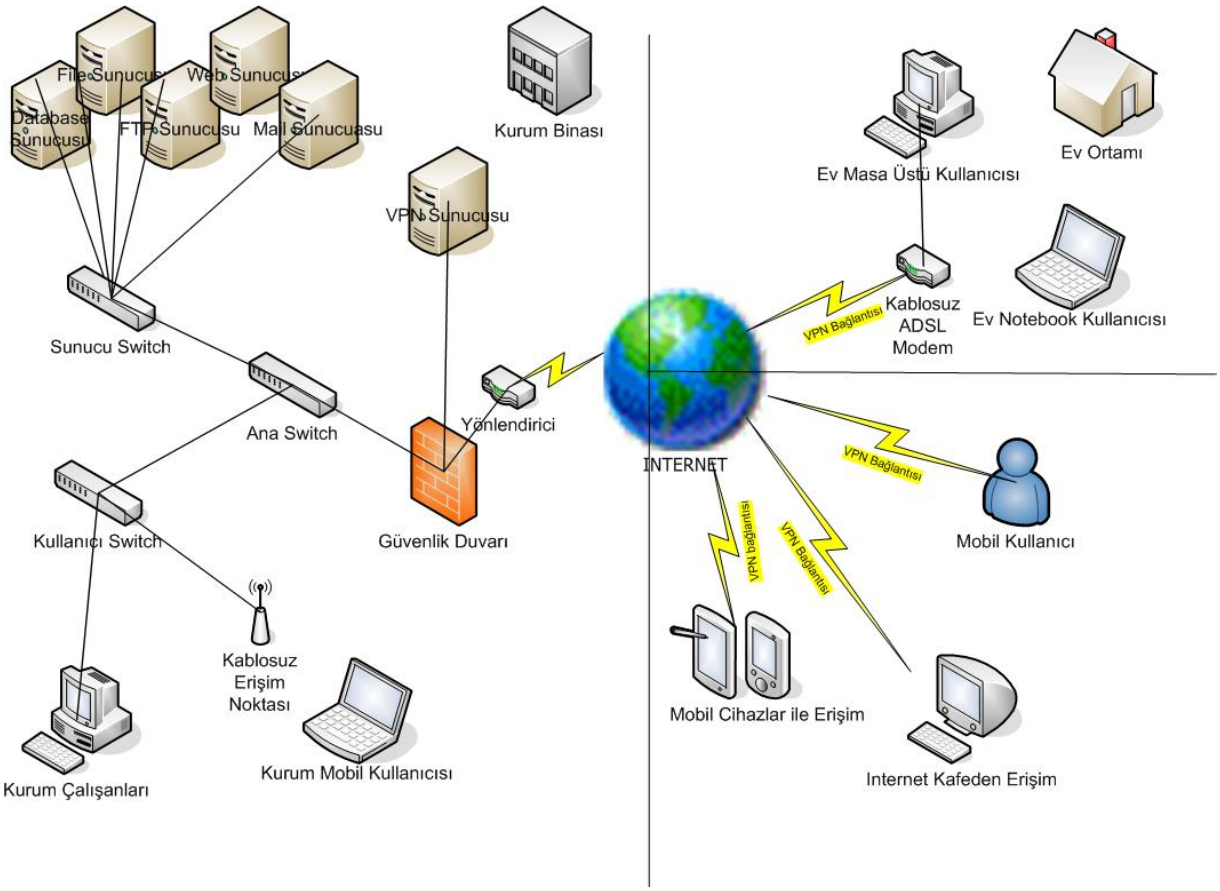
Küçük ve orta ölçekli kurum birimlerini, anahtarlar (switch) ile bağlayarak kurumdaki yazıcıları, sunucuları ve diğer kaynakları kullanmak için oluşturulan yapıdır. Bu yapıda, Internet erişimi için, temel yönlendirici ve güvenlik duvarı (router-firewall) kullanılır. Bu tür kurumlar tek bir bölgede ve tek bir yapıdan oluştukları için kurum devamlılığını sürdürebilmeleri açısından bu model yeterli olacaktır. Bu yapıya bir örnek Şekil 3.1'de verilmiştir.



Şekil 3.1. Temel kurumsal ağ modeli.

3.2.2. Büyük Bir Kurumun Ağ Yapısı

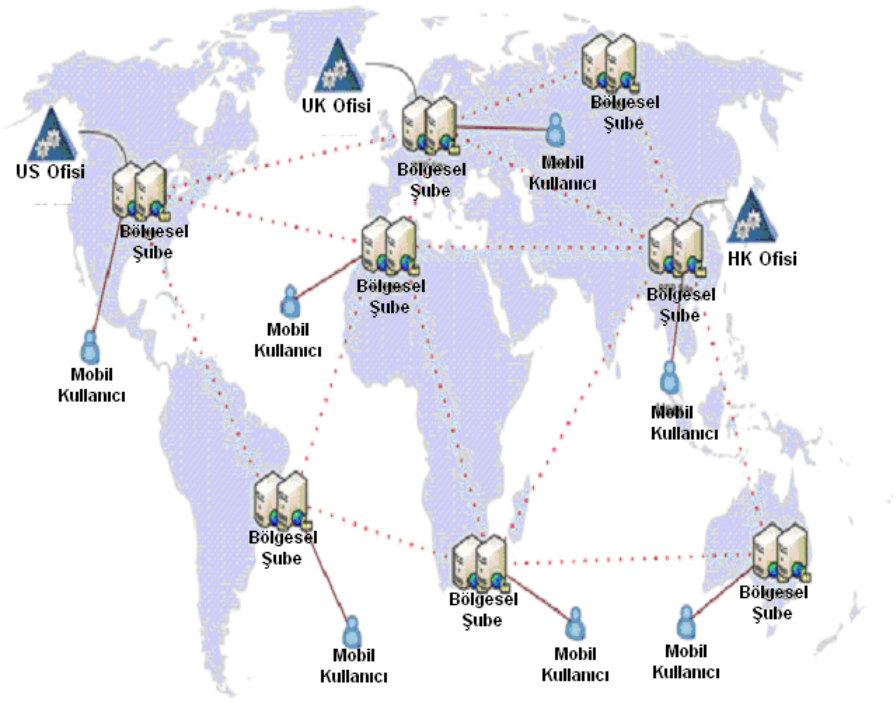
Büyük kurumlar, diğer küçük kurumlara göre, karmaşık yapıları gereği muhtemel güvenlik sorunlarının en az seviyeye düşürülmesi gereken kurumlardır. Bu tarz kurumlar, müşterilerine Internet üzerinden hizmet verebilecek, piyasalarla ve diğer kurumlarla sürekli bağlantısı olması gereken kurumlardır. Şekil 3.2'de büyük bir kurum ağ yapısına örnek verilmiştir. Bu örnekteki kurum, dışarıdan gelebilecek saldırıları önlemek için güvenlik duvarı ve tüm çalışanlarının Internet erişimini sağlamak için de vekil (proxy) sunucu kullanmaktadır. Çalışanlarının, kurum dışında bulunurken şirket ağına erişebilmeleri için bir VPN yapılandırılması kurulmuştur. İhtiyaç duyduğu posta, dosya ve genel ağ (Internet) sunucusu gibi tüm sunucularını kendi bünyesinde bulundurmakta ve güvenliğini sağlamaktadır.



Şekil 3.2. Büyük bir kurumun ağ yapısı.

3.2.3. Dağıtık Yapıdaki Bir Kurumun Ağ Yapısı

Dünyada yaşanan küreselleşme, teknolojinin gelişim hızı, oluşan yeni pazarlar, müşteri ihtiyaç ve beklentilerinin değişmesi gibi sebeplerden ötürü bir çok kurum kabuğunu kırarak çalışma alanlarını dünyanın farklı bölgelerine yaymaktadır. Kurumsal firmalardaki bu gelişmeler sonucunda ortaya çıkan iletişim ihtiyacına çözüm, dağıtık yapıdaki ağların İnternet Servis Sağlayıcılar (ISP) üzerinden gerekli ağ cihazları ile kurulan ağ yapıları olmuştur. Bu yapılara örnek Şekil 3.3'te verilmiştir.



Şekil 3.3. Dağıtık ağ yapılarına örnek.

3.3. Günümüz Kurumsal Ağ Yapılarını Oluşturan Temel Donanım Yapıları

3.3.1. Anahtar (Switch)

Anahtarlar ağ sisteminde farklı ağ bağlantı noktalarının birbirleriyle doğrudan haberleşebilmesini sağlayan ağ cihazlarıdır. Anahtarların bağlı oldukları sistemlerde anahtarlamalı bir yol ortamı sağlamalarından dolayı aynı anda birden çok iletişim kurma olanağı vardır. Böylece yüksek performans elde edilir. Anahtar, teknolojilerine göre Ethernet switch, ATM switch şeklinde isimlendirilir.

Bir anahtara bağlı kullanıcıların ve sistemlerin, kapı (port) bazında mantıksal olarak gruplandırılmasına VLAN (Virtual LAN) denir. VLAN'lar oluşturulduğunda her VLAN sadece kendi VLAN grubundaki cihazı görür, bu da güvenlik ve performans açısından büyük fayda sağlar. VLAN'lar fiziksel bir ağ üzerinde sanallaştırılarak farklı ağlar olarak oluşturulduğu için, bu ağların birbirine erişmesinde yönlendirici veya üçüncü katmanda bu görevi gerçekleştirebilecek bir cihaza ihtiyaç vardır.

VLAN'lar statik ve dinamik olmak üzere iki gruba ayrılır. Anahtarlar üzerindeki port'lara VLAN tanımı yapılarak oluşturulan yapıya statik VLAN denir. Anahtar üzerindeki bir port'a

VLAN tanımı yapıldığı zaman, değiştirildiği ana kadar o port tanımlanan VLAN'ın üyesidir. Bu yöntem ile ağı yönetmek ve izlemek daha kolaydır. Dinamik VLAN'larda ise anahtarın port'una bir cihaz takıldığı an, anahtar otomatik olarak cihazı tanır ve atanması gereken VLAN'a atar.

Anahtarlar üzerinde gelen ve giden ağ trafiğini denetleyebilmek için IP veya port bazında filtreleme yapılmasını sağlayan kontrol sistemine ACL (Access Control List) denir. ACL'ler ile ağ üzerinde kullanılması istenmeyen port'lar, anahtar üzerinden engellenebilir [11].

3.3.2. Yönlendirici (Router)

Ağdaki LAN-WAN bağlantısında veya LAN'lar arası bağlantılarda ağ paketi yönlendirme işini yapan cihazdır. OSI modelinde 3. katmanda çalışırlar. Ağ üzerindeki sistemlerin, gönderdikleri paketlerin bulundukları ağdan başka bir ağa ulaşabilmesi için yönlendiricilere ihtiyaç vardır. Paketlerin yönlendirilmesi, ağın yapısı ve gerekliliklere göre çeşitlilik göstermektedir.

Yönlendiricilerde, üzerinde gelen ve giden ağ trafiğini anahtarlar gibi denetleyebilmek için, ACL ile IP ve port filtrelemesi yapabilir. ACL'ler ile ağ üzerinde kullanılması istenmeyen portlar, daha güvenlik duvarına gelmeden yönlendirici üzerinden engellenebilir.

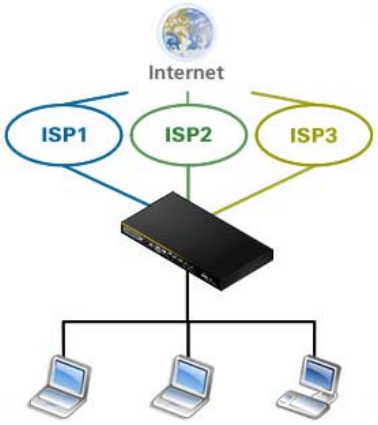
Yönlendirme üç şekilde olabilir. Yönlendirici üzerindeki yönlendirme tanımlarının elle giriş yapılarak gerçekleştirildiği, yapıda herhangi bir değişiklik olduğunda da elle müdahale edilmesi gereken yönlendirme şekline statik yönlendirme denir. Bu yapıda herhangi bir dinamik yönlendirme mümkün değildir.

Yönlendirici üzerinde yapılmış olan dinamik ve statik tanımlara uymayan taleplerin, tanımlanmış bir adrese yönlendirildiği şekle ön tanımlı yönlendirme denir. Oluşabilecek herhangi bir riske karşı ön tanımlı yönlendirme yapılarak, tanımı olmayan isteklerin ağ geçidine yönlendirilmesi her zaman önerilir.

Yönlendirici üzerinde tutulan ağ bilgilerinin, dinamik olarak güncellendiği, yönlendirme işleminin RIP, IGRP, EIGRP gibi protokollerle belirlendiği yönlendirme şekline dinamik yönlendirme denir. Bu yönlendirmede, ağ üzerindeki trafik yükünün artması ile oluşabilecek tıkanmalar ya da bağlantıların kopması nedeniyle alternatif yollar oluşturulur. Fakat dinamik yönlendirme algoritmaları; diğer algoritma yöntemlerine göre, daha karmaşıktır. Hataya dayanıklı olması beklenen sitemlerde yönlendirme tablolarının dinamik yöntemler kullanılarak oluşturulması gerekir.

3.3.3. Yük Dengeleyici

Yük dengeleyici sistemleri, aynı anda birden fazla servisin tek bir sistem gibi çalışmasını sağlayarak, sistemlerden birinde sorun yaşanması durumunda ayakta kalan diğer sistemler üzerinden devamlılık sağlayarak, kesintisiz hizmet sunumunu gerçekleştirmek ve mevcut yükü birden fazla servise dağıtmak için kullanılan donanımsal veya yazılımsal sistemlerdir. Şekil 3.4'te farklı ISP'lerden alınan Internet hizmetinin yük dengeleyici ile kullanılması gösterilmektedir.



Şekil 3.4. Yük dengeleyici ile internet erişimi.

3.4. Kurumsal Ağdaki Sunucular

Kurumsal bir ağ yapısı içersinde bir kaynağı farklı sistemlere paylaştıran sisteme sunucu denir. Kurumsal firmalar, oluşturdukları bilgi işlem merkezlerinde içersinde barındırdıkları sunucular ile şube ve kullanıcılarına hizmet sunarlar. Bundan dolayı ağ yapılarında bulunan, istemcilerden gelen isteklere cevap veren, temel hedefi; 7 gün 24 saat, kesintisiz hizmet veren sunucuların kurum açısından çok büyük önemi vardır.

3.4.1. Alan Adı Sunucusu

Ağ yapıları üzerinde bulunan sistemler ile bu sistemlerin kullandığı IP'leri birbiriyle eşleştiren sunucuya Alan Adı Sunucusu (Domain Name Server – DNS) denir. Gerçekte ağ üzerinde bulunan sistemler IP numaraları ile birbiriyle iletişim kurarlar. Eğer DNS'ler olmasaydı Internet de dahil olmak üzere tüm ağlardaki sistemlere, sayfalara ve servislere erişim IP numaraları ile gerçekleştirilecekti. DNS'ler bizim girdiğimiz adreslerin karşılığı olan IP'leri bize verir, biz de bu adresler ile talep ettiğimiz hizmeti almış oluruz.

3.4.2. Dosya Sunucusu

Kurum kullanıcılarının dosyalarının tutulduğu, dosyalar üzerinde erişim yetkilerinin tanımlandığı sunuculardır. Dosya sunucuları sayesinde kullanıcılar dosyalarına kurum ağının herhangi bir noktasından erişebilirler ve yedekleme sistemleri ile bu dosyaların yedeklerinin alınması sağlanır.

3.4.3. Posta Sunucusu

Kurum kullanıcıların kendileri arasında ve dış dünya ile mesajlaşarak, etkili bir haberleşme yapısı sağlayan sunuculara posta sunucusu denir. Bilgisayar ağ yapılarının oluşturulma sebeplerinden biri olan bir yerden diğerine bilginin gönderilmesi mantığına dayanan, temelde bir haberleşme şekli olan e-posta, bu amaçla kullanılan servislere verilen genel addır. Exchange Server, Lotus Notus Mail Server, Send Mail, Qmail ve Postfix gibi programlar sunucular üzerinde çalışan ve e-posta hizmeti veren uygulamalardır.

3.4.4. Web Sunucusu

Kurum ağında veya Internet üzerinde bulunan, kullanıcıların internet tarayıcıları aracılığıyla gönderdikleri isteklere tarayıcıların anlayacağı HTTP, HTTPS, FTP gibi standart protokollerde cevap veren, web sitelerinin yayınlandığı sunuculardır. Günümüzde en yaygın kullanılan web sunucuları Apache ve Microsft'un IIS (Internet Information Server) Web sunucularıdır. Bu web sunucularının dışında iPlanet ve NCSA'nın da web sunucuları bulunmaktadır. Netcraft tarafından yapılan istatistiklere göre kullanılan web sunucularının %54'ü Apache, % 25 IIS ve % 19'unu diğer web sunucuları oluşturmaktadır [12].

3.4.5. Vekil Sunucusu

Kullanıcılar ile Internet arasında yer alan bir aracı sunucudur. Hem Internet'te oturum açmak, hem de bir web sitesine erişimi engellemek için kullanılabilir. Kullanıcıların veya sistemlerin Internet'e erişimi için ilk önce vekil sunucudan istek yapılır, vekil sunucu istek yapılan sayfayı istek yapan kişiye döndürür.

3.4.6. DHCP Sunucusu

DHCP açılımı Dynamic Host Configuration Protocol olup, basit olarak sistemdeki bilgisayarlara IP adreslerini ve buna ek olarak değişik parametreleri atamak için kullanılan protokoldür. DHCP'nin temel özelliği sistemi kuran kişilerin tek tek tüm makineleri gezip aynı veya benzer parametreleri defalarca el ile girmesi yerine DHCP sunucusu vasıtasıyla otomatik olarak atamaktır ve böylece zaman kazanmak ve sistem yöneticisinin işini kolaylaştırmaktır.

Günümüz ağ yapılarında çok çeşitli DHCP sunucuları vardır. Bunlardan en çok kullanılanlar, Microsoft DHCP Server [13], QIP [14] ve tüm Linuxlar üzerinde gelen DHCP Server uygulaması sayılabilir.

3.5. Kurumsal Ağlardaki Güvenlik Yapıları

3.5.1. Güvenlik Duvarı

Ağ sistemlerini Internet ortamından gelecek saldırılara karşı korumak için geliştirilmiş sistemlerdir. Farklı filtreleme özellikleri ile ağda gelen ve giden paketlerin Internet trafiği kontrol edilir. IP filtreleme, port filtreleme, web filtreleme, içerik filtreleme bunlardan bazılarıdır. Güvenlik duvarları yazılımsal ya da donanımsal olabilirler. Güvenlik duvarları veri paketlerinin geçişine izin verir ya da reddeder veya vekil servisleri ve ayrıntılı inceleme yöntemleriyle ağı dışarıdan gelecek saldırılara karşı korurlar.

Güvenlik duvarlarının beş farklı türü vardır. Bunlar: Statik Paket Filtre Güvenlik Duvarı, Devre Seviyesi Güvenlik Duvarı, Durum Denetimli Güvenlik Duvarı (Stateful Inspection Firewall), Uygulama Katmanı Güvenlik Duvarı ve Vekil (Proxy) Destekli Güvenlik Duvarıdır.

Çok az kullanılmasına rağmen bazı sistemlerde yer alan Statik Paket Filtre Güvenlik Duvarları verilerin başlık kısmını okuyarak, tanımlı kurallara göre engeller veya izin verirler. Bu yapıların en büyük sorunu isteği ilk gönderen sistemi bazen tespit edememesidir.

Devre Seviyesi Güvenlik Duvarı, iletişim başladığı anda paketlerin küçük bir denetime tutulduğu, kaynak ile hedef arasında doğrudan bir bağlantı kurulmadan NAT (Network Address Translation) denen ağ adresinin farklı bir adrese dönüştürüldüğü tekniği kullanan bir mimaridir. Sistemin yerel ağdaki IP adresini dışarıya bağlı noktalardan gizler. Bu tür güvenlik duvarlarının kaynak ile hedef arasındaki paketleri analiz edememeleri en büyük eksikliğidir.

Durum Denetimli Güvenlik Duvarları (stateful inspection firewall) ise statik paket filtre güvenlik duvarlarının yetersiz kalması sonucu geliştirilmiştir. Durum kontrolleri için paketler ağ katmanında (network layer), yüksek performans açısından statik paket filtre güvenlik duvarlarında olduğu gibi filtrelenir. Daha sonra paketin bütün katmanlarına erişilerek yüksek güvenliği sağlamak için denetlenir. Bu şekilde veri kaynaktan hedefe kadar takip edilmiş olur.

Uygulama Katmanı Güvenlik Duvarları paketin başlığını incelemekle beraber paketin içeriğini de kontrol ederek paket hakkında daha fazla bilgi elde eder. Güvenlik duvarına istek gelmediği sürece tüm portlar kapalı tutulur. Günümüzde yaygın olarak kullanılmakta olan güvenlik duvarı mimarisidir.

Uygulama katmanında çalışan Vekil Destekli Güvenlik Duvarları (Proxy Based Firewall) oturumları kendileri başlatır. Kaynaktan güvenlik duvarına bir istek geldiğinde, güvenlik duvarı isteği kaynağa göndererek oturum açılır ve iletişim sürdüğü sürece bu işlem devam eder. Paket içeriğini analiz edebilmeleri Vekil Destekli Güvenlik Duvarlarının en önemli artısıdır ve kaynak ile hedef arasında yalıtım görevi yaparlar.

3.5.2. Saldırı Tespit Sistemleri

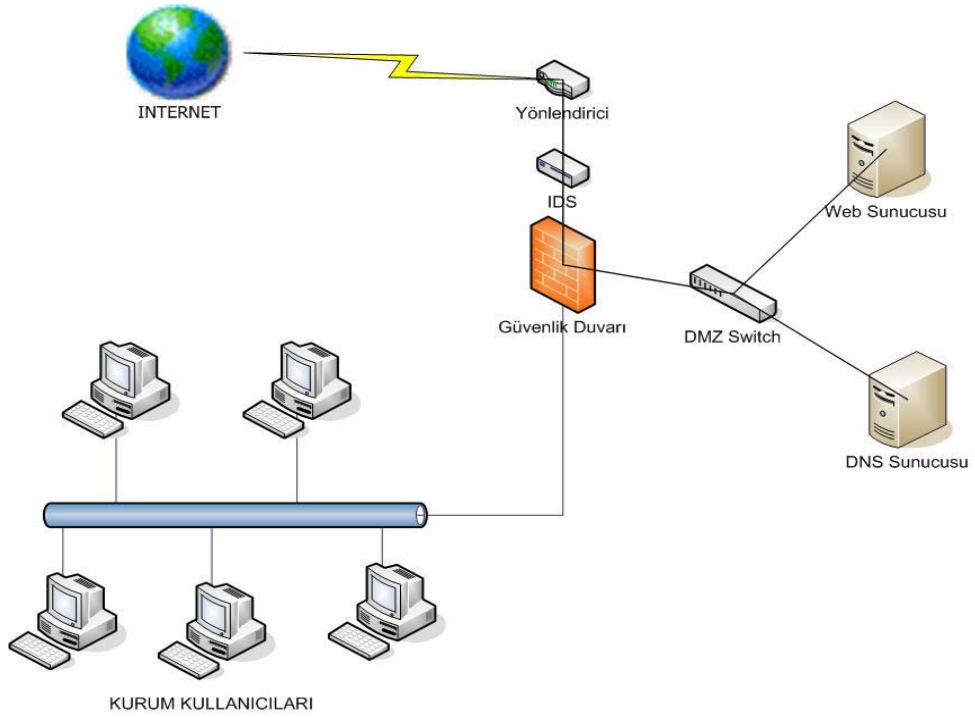
Internet'in yaygınlaşması ve Internet saldırıların da bununla beraber artması IDS'leri (Intrusion Detection System) kurum Internet güvenliği açısından önemli yapılarından birisi haline getirmiştir. Ağ tabanlı ve sunucu tabanlı olmak üzere iki türü bulunmaktadır.

Ağ tabanlı IDS'ler kurum ağına gelen tüm Internet trafiğini alarak, her bir paketi analiz edip atak olup olmadığını tespit etmektedir. Bu tespit işlemini veri tabanında tuttuğu saldırı türleriyle karşılaştırarak gerçekleştirir. Sunucu tabanlı IDS'ler ise, kurulu olduğu sunucuya gelen tüm trafiği kendi veri tabanındaki saldırı türleri ile eşleştirerek atakları engellemektedir. IDS kullanımına bir örnek Şekil 3.5'te verilmektedir. Şekilden de görülebilmeği gibi tüm Internet trafiği IDS üzerinden geçerek, oluşabilecek saldırılar engellenmeye çalışılır [15].

3.5.3. VPN

Herkesin kullanımına açık olan Internet ortamında, 'tunneling protocol' ve güvenlik yöntemleri ile iki nokta arasında şifrelenmiş bir kanal oluşturularak meydana getirilen sanal ağ teknolojisidir. VPN ile kurum ortamından uzak diğer ortamların, kurumla bağlantı yapabilmesini

sağlayarak çok ekonomik harcamalar ile hem güvenlik hem de şirket kaynaklarına ulaşılması sağlanmış olur.



Şekil 3.5. IDS kullanımı.

3.6. Modelleme ve Simülasyon

Bir sistemin ya da yapının durumunu inceleyerek gelecekteki durumu hakkında tahminlerde bulunabilmek amacıyla oluşturulmuş gerçek sistemin benzetimine modelleme denir. Simülasyon ise, gerçek bir sistemi temsil eden modelin oluşturulması işlemidir.

Simülasyonlar ile yapılan çalışmalar, problem çözme ve geliştirme yapmak için son derece etkilidir. Simülasyonlar ile değişik amaçları gerçekleştirmek için farklı alanlarda kullanılabilen, üretim, hizmet ve eğitim sektöründe yaygınlaşan bir yöntem olmuştur.

3.7. Ağ Simülasyon Araçları

3.7.1. NS-2

1989 yılında C++ ve OTcl ile geliştirilmiş olan NS-2 (Network Similator-2), ilk olarak yazılan simülasyon programıdır [16], [17]. Senaryo yazılması için kullanılan OTcl yüksek seviye tanımlamalı bir dildir. OTcl'in içerisinde yer alan kodlar alt seviyedeki modülleri çağırarak

çalışmaktadır. OTcl'e üzerinde yeni bir geliştirme gerektiğinde, geliştirme yapılan kodun mantığı alt modülünde C++ ile yazılması gerekmektedir.

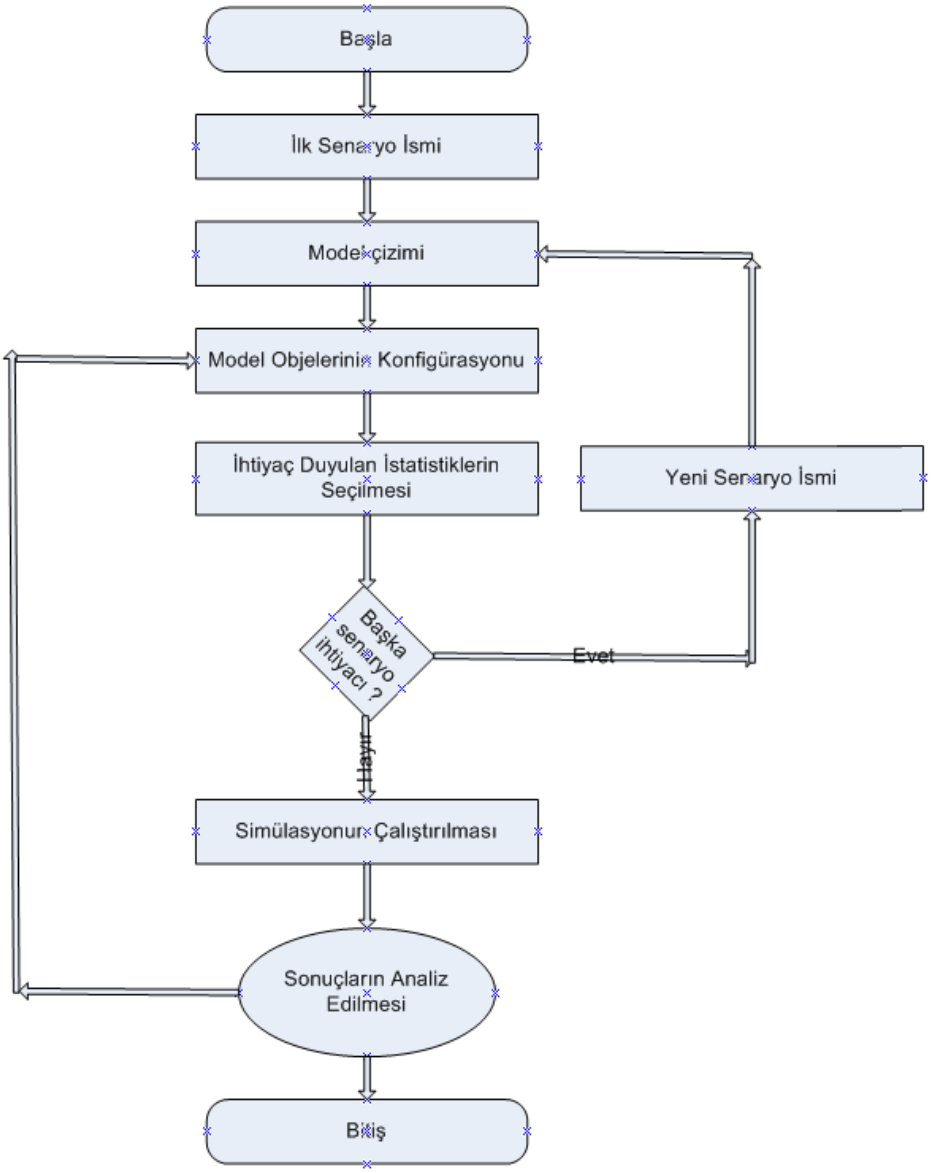
NS-2 farklı büyüklükteki ağların simülasyonunda kullanılabilmektedir. NS-2 benzetim analizi sonucunda iki ayrı çıktı elde edilmektedir. Birinci çıktı, tarihçe dosyası olarak isimlendirilen ".tr" uzantılı "trace files" dosyalarıdır. İkinci çıktı olan NAM (Network Animatör) dosyası ise geliştirilen programın kodlarına göre algılayıcıların durumunu, paket içeriklerini kısacası tarihçe dosyası içerisindeki bilgileri görsel olarak görmeyi sağlamaktadır.

3.7.2. OPNET Yazılımı

OPNET, ağ ve ağ cihazlarının, uygulama sunucuları ile modellenerek benzetimlerinin yapılmasına sağlayan bir yazılımdır [18], [1]. OPNET ile ağ teknolojileri, uygulamalar, çeşitli bileşenlerle sanal ortamlar oluşturularak analizler yapılır. OPNET gibi simülatörler ile yapı oluşturmak, gerçek kaynaklarla oluşturmaktan daha ucuzdur. Endüstride OPNET'in ana kullanılma sebepleri, benzetim maliyet düşüklüğü ve gerçek sistemler üzerinde deney yapmanın imkânsızlaşmasıdır. Gerçek yapılara benzer modeller üzerinde geliştirme yapmak, para ve zaman tasarrufu sağlar. OPNET, dünya üzerinde binlerce ticari kuruluş ve bunun yanında 500'den fazla üniversite tarafından kullanılmaktadır.

OPNET yazılımı, TCP/IP, ATM, frame relay, MPLS, IP gibi ağ protokollerinin ve 3Com, Cisco, Bays Network gibi üreticilerin üretmiş olduğu anahtar ve yönlendirici gibi ürünlerin modellerinin yer aldığı geniş bir kütüphaneye sahiptir. OPNET'in en büyük avantajlarından bir tanesi; kullanıcıların yeni protokol ve ürünlerin modellerini oluşturabilmesidir.

OPNET istenilen boyuttaki ağlarda simülasyon yapmaya imkan sağlar. Ofis boyutunda bir ağ simülasyonu yapılabileceği gibi, dünya üzerindeki farklı bölgelerde bir proje oluşturmak da mümkündür. Oluşturulan projenin simülasyon süresi değiştirilerek gerçekleştirilmesi mümkündür. Bu özellikler, OPNET uygulamasının gerçeğe yakın simülasyonlar oluşturduğunun bir göstergesidir. Şekil 3.7'de OPNET'te ağ modelleme akış diyagramı görülmektedir [4].



Şekil 3.7. OPNET ile ağ modelleme akış diyagramı.

i. OPNET uygulaması ile bir ağ modeli oluşturularak başlanır.

ii. Yeni model oluşturulurken, yeni bir proje ve yeni bir senaryo oluşturulması gerekir.

iii. İlk senaryo oluşturulduktan sonra, OPNET'in sunduğu protokoller ve desteklediği ürünler ile model çizimi yapılır.

iv. Çizilen model üzerindeki protokollerin ve ürünlerin VLAN ve Güvenlik Duvarı gibi özellikleri düzenlenir.

v. Hazırlanan modelde örnek olarak HTTP cevap süresi (response time), sunucudaki ana işlem biriminin (CPU) kullanımı gibi toplanması istenen bilgiler belirlenerek seçilir.

vi. Birden fazla senaryoyu karşılaştırma ihtiyacına göre madde ii'deki akışa dönülerek yeni bir senaryo oluşturulur.

vii. Hazırlanan model üzerindeki simülasyonlar çalıştırılır.

viii. Çalıştırılan simülasyonların çıktıları tek tek veya karşılaştırma özelliği ile analiz edilir. Sonuçların yeterliliği ve çıktıların doğruluğuna göre madde vi'e geri dönülerek ürünlerin ve protokollerin özellikleri düzenlenir.

ix. Simülasyon çıktıları yeterli olduğu kabul edilerek çalışma bitirilir.

Bir sonraki bölümde büyük bir kurumu ve tipik güvenlik unsurlarını dikkate alarak, yukarıda sunulan temel ağ yapıları ile bir kurum ağı modeli oluşturulacaktır.

4. GERÇEK VE SİMÜLASYON ORTAMLARININ TASARLANMASI VE ANALİZİ

4.1. Giriş

Bu bölümde bir kurumsal ağı tasarlayarak, hem gerçek ortamda hem de OPNET simülasyon ortamında oluşturacağız. Gerçek olarak oluşturduğumuz donanım ortamında testler yaparak daha sonra OPNET ortamından aldığımız sonuçlar ile karşılaştırmalar yapacağız.

4.2. Gerçek Ortamı Analiz Etmede Kullanılan Araçlar

Kurumsal ağ yapılarının, ağ analiz araçları ve sistem izleme araçları ile testler yapılarak incelenmesi, kurumların güvenlik ve performans açıklarını kapatmaları konusunda yardımcı olan çalışmalardır. Ağ yazılım teknolojilerindeki ilerlemeler ile günümüzde analiz kabiliyeti çok yüksek çok fazla sayıda araç geliştirilmiştir. Bu araçların bir kısmı ücretli ürünler olup bir kısmı da gönüllü grupların geliştirdiği ücretsiz sistem araçlarıdır. Bu çalışmalarda kullanılan sistem araçlarına örnekler Wireshark [19], Softperfect Network Protocol Analyzer [20], NMAP-Network Security Scanner [21], Grinder [22], Apache Jmeter [23] ve CACE Pilot [24] sayılabilir.

4.2.1. Apache JMeter – Stres Test Aracı

Apache JMeter Java dilinde yazılmış stres test aracı olarak kullanılan bir uygulamadır. İlk başlarda web sunucuları için tasarlanan bir test aracı olsa da, sonrasında başka test alanlarında da başarılı olmuştur. Apache JMeter hem durağan (static) hem de değişken (dynamic) kaynakları test etmek için kullanılabilir. Bir sunucu üzerinde ağır yükü (heavy load) simüle edip, değişik yükler (load) için genel performansını gözlemek için kullanılabilir. Sonuçları analize etmek için Apache JMeter değişik grafiksel çizimleri oluşturabilir.

JMeter, HTTP, FTP ve veri tabanı sunucuları (JDBC kullanarak) üzerine ağır yük ve performans testleri yürütebilir. 100% Java dilinde yazılmış olduğundan platformdan bağımsız taşınabilirdir. Çok-thread'li bir yapıya sahip olduğundan, birkaç fonksiyonu aynı anda yapabilmekte ve çok kullanıcılı bir ortamı simule edebilmektedir. Çevrim dışı (offline) olarak web sitlerini gözlemlemekte ve analiz edebilmektedir. Genişleyebilir olmasından eklenebilen fonksiyonlar ile sonsuz test imkanları sağlamaktadır.

Biz JMeter'i çalışmamızda, belirli bir zaman aralığı içerisinde rasgele (random) olarak, web sunucusuna HTTP istekleri göndermek için kullanacağız.

4.2.2. Wireshark – Paket Toplama Aracı

Wireshark, çok güçlü özelliklere sahip açık kaynaklı ağ paket analiz yazılımıdır. Wireshark bir ağa karşı yapılacak bir saldırı durumunda uyarılarda bulunacak bir saldırı tespit sistemi değildir. Farklı bir durum oluştuğunda toplanacak veriler ile sorunun ne olduğunu fark etmeye yardımcı olur. Wireshark en başarılı ağ protokol analizcilerinden biri olarak kabul edilir ve çoğu endüstri ve eğitim enstitüsünde standart sayılmaktadır. Wireshark bu kadar başarılı olması, 1998 yılından itibaren dünyanın farklı yerlerindeki ağ uzmanlarının yazılımın geliştirilmesine katkıda bulunması nedeniyledir.

Wireshark'ın dikkat çeken özellikleri, 750'nin üzerinde protokolü analizi, gerçek zamanlı analiz kabiliyeti, analiz filtre özelliği, Windows, Linux, OS X, Solaris, FreeBSD, NetBSD ve bir çok işletim sisteminde çalışabilmesi, zengin VoIP analizleri yapabilmesi, birçok yakalama dosya biçimini yazıp okuyabilmesi, IPSec, WPA gibi birçok protokol için şifre çözme desteği sunabilmesi ve çıktıları XML, PostScript, CSV, veya düz metin seklinde verebilmesi şeklinde sıralanabilir.

Wireshark'ı oluşturacağımız gerçek kurumsal ağ modelinde bir sunucu üzerinde çalıştırarak, testlerimiz sırasında oluşacak ağ paketlerini toplamak için kullanacağız.

4.2.3. CACE Pilot – Paket Analiz Aracı

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'un Wireshark ile birlikte çalışması verimliliği artırırken, kullanıcıların mevcut uzmanlığını geliştirerek, ağ problemlerinin anlamak ve belirlemek, ağ performansını ölçme konularında yardımcı olur.

Kısa bir sürede içerisinde gigabyte'lar seviyesindeki dosyaların izlenebilmesi ve analizi, istenilen ağ parametreleri kullanılarak filtrelere koyulabilmesi ve yalıtılan trafiğin daha kolay analiz edebilmesi, ağ trafik istatistiklerini görsel olarak sunabilmesi, uzun süreli ağ trafiğini izlemesi ve raporlayabilmesi en belirgin özellikleri olarak sayılabilir.

Cace Pilot uygulamasını, Apache Jmetter ile yaptığımız testler sırasında Wireshark ile topladığımız ağ paketlerini analiz etmek için kullanacağız.

4.2.4. Windows Performans Monitör

Microsoft'un tüm işletim sistemlerinde sunduğu Performans Monitör aracı, sunucular üzerinde çalışan birçok nesneyi değişik kriterlere göre analiz edilmesine imkan sağlar. Örnek olarak "Web Service instins" nesnesinin altında bulunan web sitesi objesinin saniyede alınan, gönderilen, toplam alınan-gönderilen veri miktarı gibi değişik sayaçlar vasıtası ile web servisinin çalışmasını ve performansını izlenebilmesine imkan sağlanır.

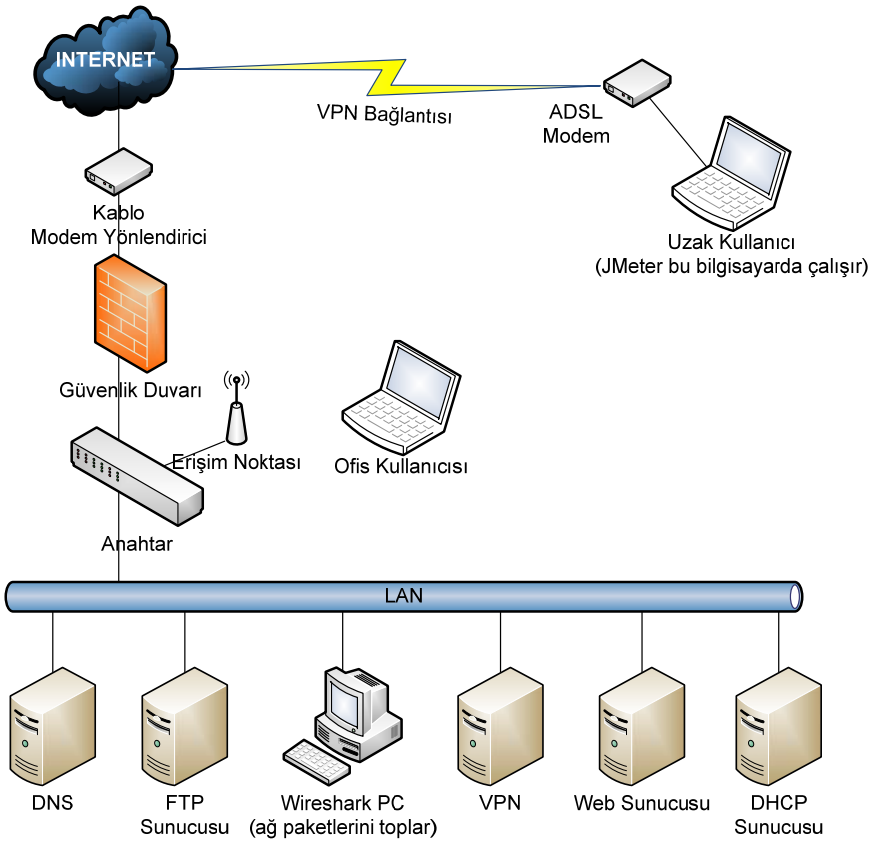
JMeter ile yaptığımız testler sırasında web sunucusu üzerinde performans durumunu Performans Monitör aracı ile izlemek için kullanacağız.

4.3. Gerçek Kurumsal Ağ Modelinin Tasarlanması ve Ayarları

Günümüz kurumsal ağ yapıları güvenlik ve verimlilik dikkate alınarak oluşturulduğunda belirli ağ cihazları ve uygulama sunucularından oluşmaktadır. Tezimizdeki gerçek kurumsal ağ modelinin tasarımında ve gerçekleştirilmesinde en temel kurum ağı bileşenleri kullanılmıştır. Tasarlanan yapı iki farklı noktadan oluşmaktadır. Birinci nokta kurumsal sunucuların yer aldığı kurumsal ağ, ikinci nokta ise ADSL bağlantısı ile VPN bağlantısı üzerinden kurum ağına ulaşıldığı uzak bağlantının olduğu noktadır. Modelimizdeki ağ yapısında anahtar ve kablosuz erişim noktası olarak Airties RT-211 ADSL Modem, Internet erişimi için NETMASTER CXC-150 Kablo Modem, Linux IPTables güvenlik duvarı, Linux OPENVPN sanal özel ağ sunucusu, 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. Uzak ev bağlantısı için ise Airties RT-201 ADSL Modem ve Windows XP Kullanıcı PC'si bulunmaktadır. Şekil 4.1'de tasarlanan kurumsal ağ yapısı yer almaktadır.

4.3.1. Güvenlik Duvarı - IPTables

Güvenlik duvarı, Internet ve yerel ağ trafiğinin, kontrol ve denetlemesini yapan yazılımdır. Güvenlik Duvarı sayesinde Internet ve yerel ağ üzerinden belirli portlar, ya da belirli IP adresi veya ip gruplarının erişimini engelleyebiliriz.

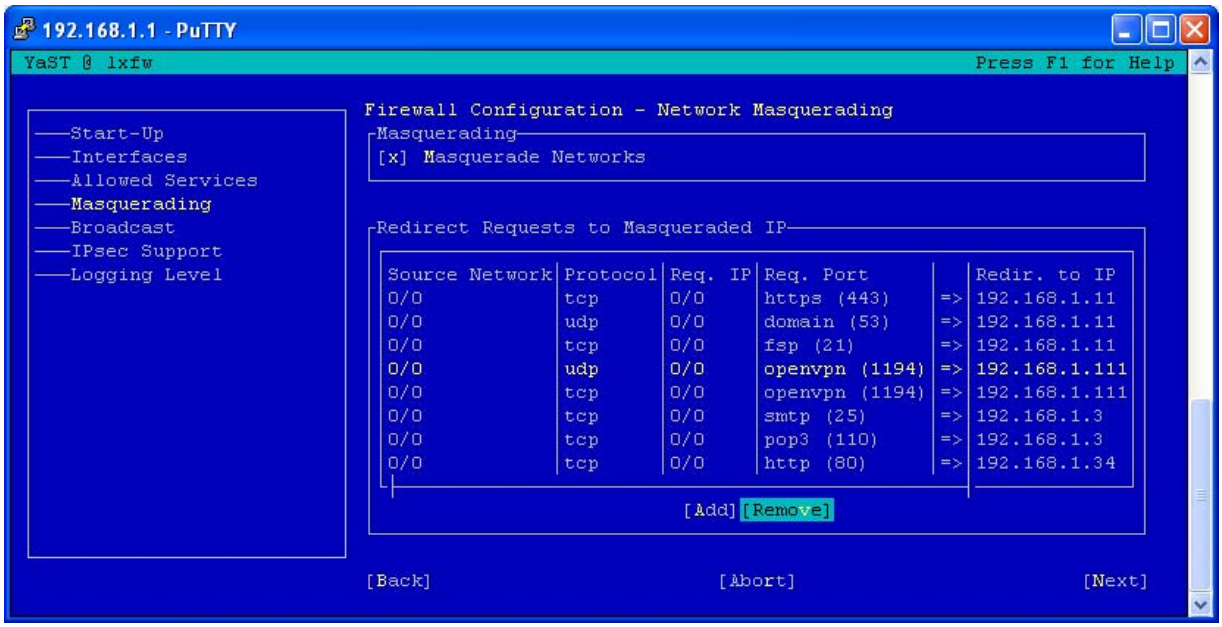


Şekil 4.1. Tasarlanan kurumsal ağ yapısı.

Kurumsal ağ modelimizde güvenlik duvarı olarak IPTables kullanılmaktadır. IPTables, neredeyse tüm Linux sürümleri ile birlikte hazır gelmektedir. Kurumsal ağ yapımızda, IPTables'i en başarılı Linux sürümlerinden biri olan Open Suse 11 [25] üzerinde çalışmaktadır.

IPTables, genişleme paketleri sayesinde birçok özelliği de sağlayabilir. Özellikle iproute2 paketi ile beraber kullanıldığında routing ve QOS özellikleriyle birlikte ücretli bir çok güvenlik duvarı ürününün özelliklerinden fazlasını sağlar. Snort gibi yazılımlarla beraber kullanarak IPS ve IDS gibi özellikleri elde etmeyi sağlar [26].

Kullanmakta olduğumuz güvenlik duvarımızın iki tane arabirimi bulunmaktadır. Birinci arabirim dış dünyadan gelen isteklere cevap verirken ikinci arabirim yerel ağa bağlanmaktadır. Dış dünyadan gelen istekleri ilgili sunucuya yönlendirmek için Maskeleme (Masquerading) özelliğini kullanmaktayız. Bu özellik, Internet ortamından gelen istekleri tanımlarına bakarak, uygunsa yerel ağdaki ilgili sunucuya yönlendirmesi şeklinde çalışır. Şekil 4.2'de kurumsal ağ üzerinde oluşturduğumuz kurallar görülmektedir.



Şekil 4.2. Güvenlik duvarı maskeleme kuralları.

4.3.2. Sanal Özel Ağ - OpenVPN

Sanal Özel Ağ Internet üzerinden şifreli ve güvenli veri iletişimi sağlamak için kullanılan bir teknolojidir. Kurumsal ağ modelimizde, sanal özel ağ çözümü olarak OpenSuse 11 üzerinde OpenVPN [27] kullanılmaktadır.

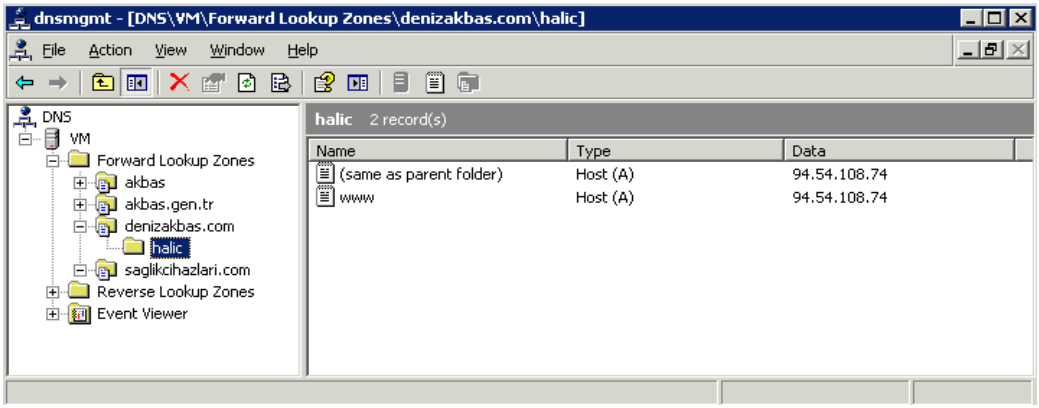
OpenVPN çoklu platform SSL VPN çözümü olup SSL/TLS protokollerini kullanarak ISO 2. ve 3. katman seviyesinde şifreli ağ erişimi sağlar. OpenVPN ile Linux, Windows 2003 ve üzeri, Mac OS X ve Solaris işletim sistemlerinde çalıştırılabilir. OpenSSL kütüphanesinin sunduğu şifreleme ve sertifikasyon özelliklerini kullanabilmesi, ağ adres dönüştürme üzerinden sorunsuz tünelleme imkanı, grafik ara yüz ile yönetim desteği, kablosuz ağlar için güvenli erişim imkanı sağlanabilmektedir.

Gerçekleştirilen kurumsal ağ modelinde, kurum dışarısında bulunan ve kurum kaynaklarına erişmek isteyen kullanıcılar için, yerel ağda bulunan bir sunucu üzerinde OpenVPN kurulumunu gerçekleştirerek, kullanıcılar için oluşturduğumuz sertifikaların kullanımı ile kurum ağına erişim sağlandı. Aşağıda VPN bağlantısı sırasında gerçekleşen iletişime bir örnek verilmiştir.

```
Mon Jul 05 00:24:27 2010 OpenVPN 2.1.1 i686-pc-mingw32 [SSL] [LZO2] [PKCS11] built on Dec 11 2009
Mon Jul 05 00:24:27 2010 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-
defined scripts or executables
Mon Jul 05 00:24:27 2010 LZO compression initialized
Mon Jul 05 00:24:27 2010 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Mon Jul 05 00:24:27 2010 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
Mon Jul 05 00:24:27 2010 Local Options hash (VER=V4): '41690919'
Mon Jul 05 00:24:27 2010 Expected Remote Options hash (VER=V4): '530fdded'
Mon Jul 05 00:24:27 2010 Socket Buffers: R=[8192->8192] S=[8192->8192]
Mon Jul 05 00:24:27 2010 UDPv4 link local: [undef]
Mon Jul 05 00:24:27 2010 UDPv4 link remote: 192.168.1.111:1194
Mon Jul 05 00:24:27 2010 TLS: Initial packet from 192.168.1.111:1194, sid=f78e9f34 b712cda4
Mon Jul 05 00:24:27 2010 VERIFY OK: depth=1,
/C=TR/ST=CA/L=SanFrancisco/O=akbas.gen.tr/OU=IT/CN=akbas.gen.tr/emailAddress=denizakb@hotmail.com
Mon Jul 05 00:24:27 2010 VERIFY OK: nsCertType=SERVER
Mon Jul 05 00:24:27 2010 VERIFY OK: depth=0,
/C=TR/ST=CA/L=SanFrancisco/O=akbas.gen.tr/OU=IT/CN=akbas.gen.tr/emailAddress=denizakb@hotmail.com
Mon Jul 05 00:24:28 2010 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Mon Jul 05 00:24:28 2010 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Mon Jul 05 00:24:28 2010 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Mon Jul 05 00:24:28 2010 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Mon Jul 05 00:24:28 2010 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit
RSA
Mon Jul 05 00:24:28 2010 [akbas.gen.tr] Peer Connection Initiated with 192.168.1.111:1194
Mon Jul 05 00:24:30 2010 SENT CONTROL [akbas.gen.tr]: 'PUSH_REQUEST' (status=1)
Mon Jul 05 00:24:30 2010 PUSH: Received control message: 'PUSH_REPLY,route 192.168.1.0
255.255.255.0,route 10.8.0.0 255.255.255.0,topology net30,ping 10,ping-restart 120,ifconfig
10.8.0.6 10.8.0.5'
Mon Jul 05 00:24:30 2010 OPTIONS IMPORT: timers and/or timeouts modified
Mon Jul 05 00:24:30 2010 OPTIONS IMPORT: --ifconfig/up options modified
Mon Jul 05 00:24:30 2010 OPTIONS IMPORT: route options modified
Mon Jul 05 00:24:30 2010 ROUTE default_gateway=192.168.1.1
Mon Jul 05 00:24:30 2010 TAP-WIN32 device [Local Area Connection 6] opened: \\.\Global\{3A83F6CE-
9C55-4F05-BB6A-AB298567A708}.tap
Mon Jul 05 00:24:30 2010 TAP-Win32 Driver Version 9.6
Mon Jul 05 00:24:30 2010 TAP-Win32 MTU=1500
Mon Jul 05 00:24:30 2010 Notified TAP-Win32 driver to set a DHCP IP/netmask of
10.8.0.6/255.255.255.252 on interface {3A83F6CE-9C55-4F05-BB6A-AB298567A708} [DHCP-serv:
10.8.0.5, lease-time: 31536000]
Mon Jul 05 00:24:30 2010 Successful ARP Flush on interface [2] {3A83F6CE-9C55-4F05-BB6A-
AB298567A708}
Mon Jul 05 00:24:35 2010 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Mon Jul 05 00:24:35 2010 Route: Waiting for TUN/TAP interface to come up...
Mon Jul 05 00:24:40 2010 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up
Mon Jul 05 00:24:40 2010 WARNING: potential route subnet conflict between local LAN
[192.168.1.0/255.255.255.0] and remote VPN [192.168.1.0/255.255.255.0]
Mon Jul 05 00:24:40 2010 C:\WINDOWS\system32\route.exe ADD 192.168.1.0 MASK 255.255.255.0
10.8.0.5
Mon Jul 05 00:24:40 2010 Route addition via IPAPI succeeded [adaptive]
Mon Jul 05 00:24:40 2010 C:\WINDOWS\system32\route.exe ADD 10.8.0.0 MASK 255.255.255.0 10.8.0.5
Mon Jul 05 00:24:40 2010 Route addition via IPAPI succeeded [adaptive]
Mon Jul 05 00:24:40 2010 Initialization Sequence Completed
```

4.3.3. Alan Adı Sunucusu – Microsoft DNS Server

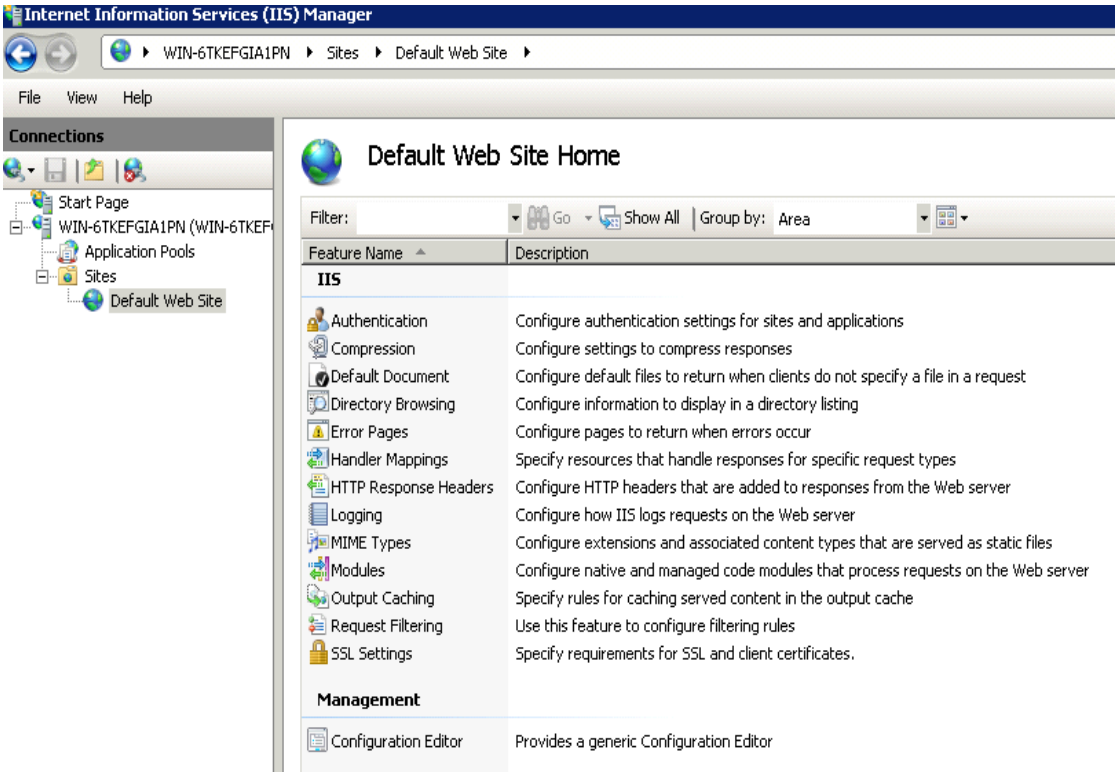
Kurumsal ağ modelimizde alan adı sunucusu olarak Windows 2003 üzerinde Microsoft DNS Server [28] kullanılmaktadır. Modelimizde yerel ağdaki Windows 2003 Sunucusu üzerindeki Microsoft DNS Server üzerinde web server için gerekli tanımlamalar yapılarak Internet'ten ve yerel ağdan web sunucusuna erişim sağlanmış olur. Şekil 4.3'te DNS sunucusu üzerinde **`halic.denizakbas.com`** alan adının tanımı görülmektedir.



Şekil 4.3. DNS sunucusu üzerinde alan adı tanımlaması.

4.3.4. Web ve FTP Sunucusu – Microsoft IIS Server

Kurumsal ağ modelimizde Windows 2008 sunucusu üzerinde çalışan IIS 7.0 Web ve FTP sunucuları kullanılmaktadır. Şekil 4.4'te IIS sunucusunun ayarları görülmektedir.



Şekil 4.4. Web sunucusu IIS 7.0'ın ayarları.

4.4. Kurumsal Ağ Modeli Üzerinde Oluşturulan Test Senaryosu

Web sunucuları http protokolü ile hizmet verirler. Birçok İnternet protokolünde olduğu gibi bu protokol de istemci-sunucu haberleşme modeliyle çalışır. İstemci sunucuya istek gönderir, sunucu da bu istekleri yorumlayarak istemciye istenen web nesnelerini gönderir..

Test işlemini, Internet üzerinden kurulan sanal özel ağ bağlantısı aracığıyla uzak bağlantı ile gerçekleştireceğiz. Oluşturduğumuz uzak bağlantı ile JMeter uygulaması üzerinden 30 sn aralılarla IIS 7.0 Web sunucusuna istekler göndermek şeklinde gerçekleştireceğiz. Test süresi 10 dk olarak belirlenmiş olup, test sırasında Wireshark aracılığıyla ağ paketleri ve Performans Monitör ile de sunucu üzerindeki performans bilgileri toplanmıştır.

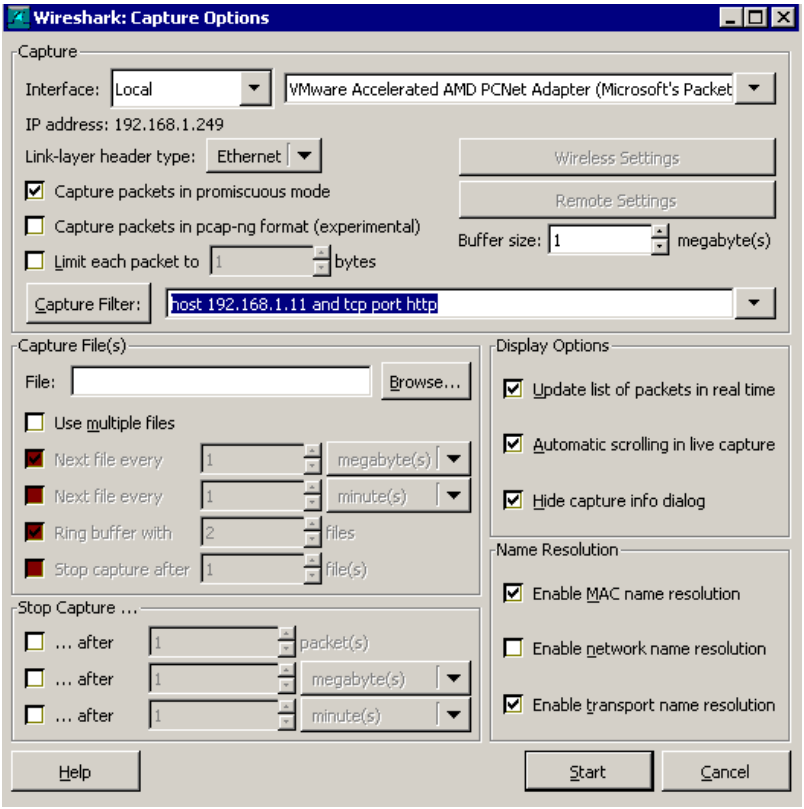
4.5. Kurumsal Ağ Modeli Üzerinde Alınan Test Sonuçları

Test işlemini, Internet üzerinden kurulan sanal özel ağ bağlantısı aracığıyla uzak bağlantı ile gerçekleştireceğiz. Oluşturduğumuz uzak bağlantı ile JMeter uygulaması üzerinden 20 ile 40 sn arasında rasgele olarak IIS 7.0 Web sunucusuna istekler göndermek şeklinde gerçekleştireceğiz. Test süresi 10 dk olarak belirlenmiş olup, test sırasında Wireshark aracılığıyla ağ paketleri ve performans monitör ile de sunucu üzerindeki performans bilgileri toplanmıştır.

4.5.1. Wireshark ile Toplanmış Ağ Paket Bilgileri

Testler sırasında yerel ağdaki Windows XP PC üzerine kurulan Wireshark uygulaması ile ağ paketleri toplanmıştır. Test sonuçlarının ve analizlerin daha iyi anlaşılır olabilmesi için Şekil 4.5'ten de görülebileceği gibi, Wireshark programında kullanılan ağ kartı üzerinde, web sunucusunun IP'si (192.168.1.11) HTTP (80) port'una gelen istekler filtrelenmiştir.

Gerçekleştirilen 10 dk test sonucunda Wireshark ile toplanan ilk 10 ve son 10 paketin özeti aşağıda yer almaktadır. Bu özette isteği yapan kişinin IP'si isteğin yapıldığı hedef IP, iletişim türü ve paket bilgisi yer almaktadır. 10 dk test süresince 200 tane ağ paketi toplanmıştır.



Şekil 4.5. Wireshark ile filtre tanımı.

No	Zaman	Kaynak Ip	Hedef Ip	Protokol	Bilgi
1	0	94.54.108.36	192.168.1.11	TCP	62343 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8
2	0,000113	192.168.1.11	94.54.108.36	TCP	http > 62343 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0
3	0,02815	94.54.108.36	192.168.1.11	TCP	62343 > http [ACK] Seq=1 Ack=1 Win=17408 Len=0
4	0,029011	94.54.108.36	192.168.1.11	HTTP	GET / HTTP/1.1
5	0,029201	192.168.1.11	94.54.108.36	HTTP	HTTP/1.1 200 OK (text/html)
6	0,259868	94.54.108.36	192.168.1.11	TCP	62343 > http [ACK] Seq=236 Ack=1178 Win=16128 Len=0
7	10,052173	94.54.108.36	192.168.1.11	TCP	62343 > http [FIN, ACK] Seq=236 Ack=1178 Win=16128 Len=0
8	10,05223	192.168.1.11	94.54.108.36	TCP	http > 62343 [ACK] Seq=1178 Ack=237 Win=65300 Len=0
9	10,052293	192.168.1.11	94.54.108.36	TCP	http > 62343 [FIN, ACK] Seq=1178 Ack=237 Win=65300 Len=0
10	10,076122	94.54.108.36	192.168.1.11	TCP	62343 > http [ACK] Seq=237 Ack=1179 Win=16128 Len=0
191	571,558552	94.54.108.36	192.168.1.11	TCP	62367 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=8
192	571,558644	192.168.1.11	94.54.108.36	TCP	http > 62367 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0
193	571,578874	94.54.108.36	192.168.1.11	TCP	62367 > http [ACK] Seq=1 Ack=1 Win=17408 Len=0
194	571,579188	94.54.108.36	192.168.1.11	HTTP	GET / HTTP/1.1
195	571,579229	192.168.1.11	94.54.108.36	HTTP	HTTP/1.1 200 OK (text/html)
196	571,800891	94.54.108.36	192.168.1.11	TCP	62367 > http [ACK] Seq=236 Ack=1178 Win=16128 Len=0
197	581,585788	94.54.108.36	192.168.1.11	TCP	62367 > http [FIN, ACK] Seq=236 Ack=1178 Win=16128 Len=0
198	581,58584	192.168.1.11	94.54.108.36	TCP	http > 62367 [ACK] Seq=1178 Ack=237 Win=65300 Len=0
199	581,585908	192.168.1.11	94.54.108.36	TCP	http > 62367 [FIN, ACK] Seq=1178 Ack=237 Win=65300 Len=0
200	581,605451	94.54.108.36	192.168.1.11	TCP	62367 > http [ACK] Seq=237 Ack=1179 Win=16128 Len=0

4.5.2. CACE Pilot Uygulaması Analiz Sonuçları

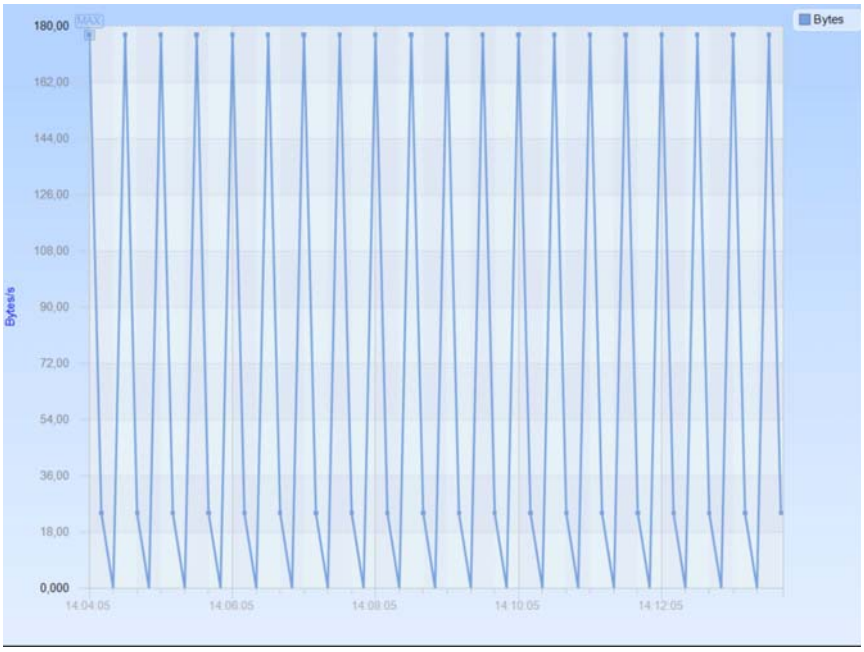
Wireshark ile toplan ağ paketlerinin CACE Pilot ile analiz sonuçları aşağıda verilmektedir:

İstatistik İsmi	Değer
Toplam Bit Miktarı	321,920
Toplam Byte Miktarı	40,240
Toplanan paket sayısı	200
Ip Protokolü Byte Miktarı	40,240
TCP Protokolü Byte Miktarı	40,240
UDP Protokolü Byte Miktarı	0

Adres	İstek Sayısı	Toplam İstek Büyüklüğü	Sunucu-Kullanıcı Büyüklüğü
halic.denizakbas.com	20	32,800	24,620

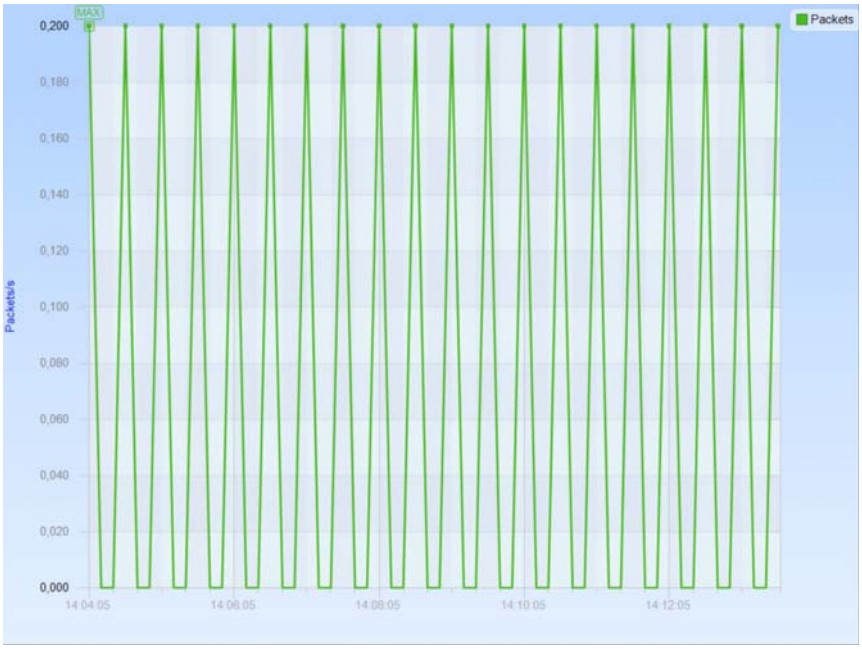
Adres	İstek Sayısı	Ortalama İstek Yanıt Süresi	En Düşük Yanıt Süresi
halic.denizakbas.com	20	609ms	41ms

Saniyede gönderilen byte miktarı - toplam bant genişliği: 600 saniye içerisinde, kullanılan bant genişliğinin grafiği şekil 4.6'da yer almaktadır. Analiz sonucuna göre, Apache JMeter ile yapılan 20 istek gözlenmektedir ve maksimum kullanılan bant genişliği 175 byte'tır.



Şekil 4.6. Kullanılan bant genişliği – byte/zaman.

Saniyede gönderilen paket miktarı - toplam bant genişliği: 600 saniye içerisinde, kullanılan bant genişliğinin gönderilen paket miktarı ile grafiği şekil 4.7'de yer almaktadır. Analiz sonucuna göre maksimum 0,200 paket gözlenmektedir.



Şekil 4.7. Kullanılan bant genişliği – paket/sn.

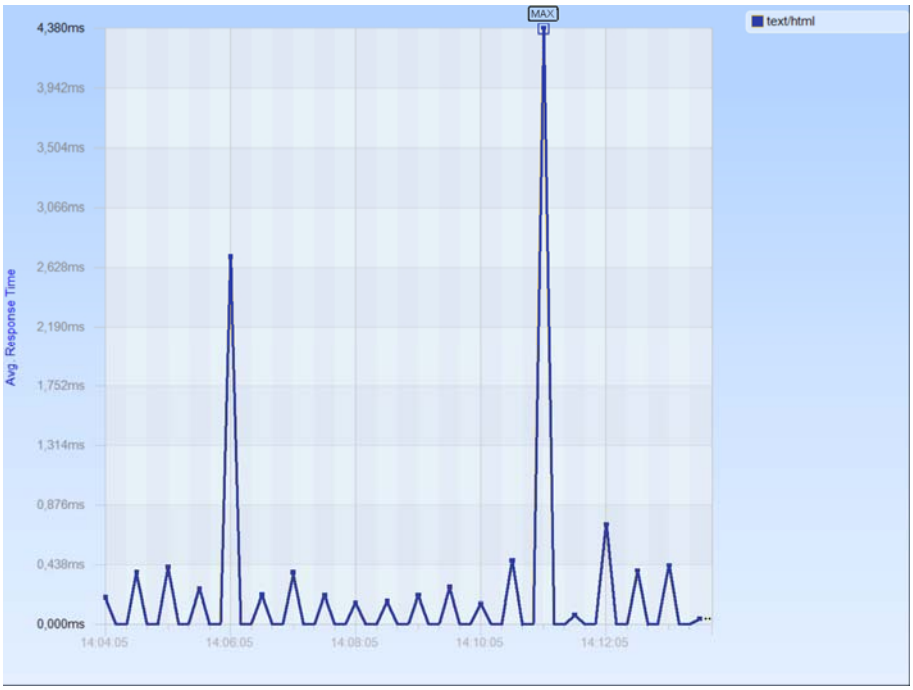
Web sunucusunun cevap süreleri: Web sunucusunun 600 saniye içerisindeki, isteklere verdiği cevapların süreleri Şekil 4.8'de yer almaktadır. Analiz sonucuna göre maksimum 4.380 ms genel olarak isteklere 0.2 ms sürelerde cevap verilmektedir.

4.5.3. Windows Performans Monitör Analiz Sonuçları

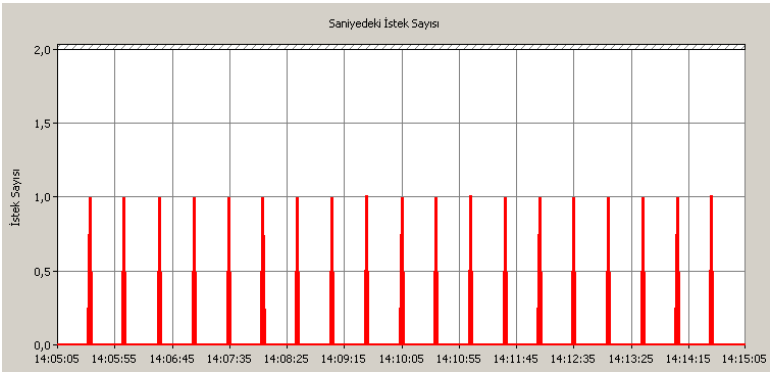
Apache JMeter ile gönderilen isteklerin Web Sunucusu üzerinde oluşturduğu etkiyi ölçmek için Windows'un Performans Monitör aracı ile toplanan analiz sonuçları aşağıda yer almaktadır.

Saniyedeki web sunucusuna yapılan istek sayısı: Web sunucusu'na 600 saniye içerisinde, gelen isteklerin durumu şekil 4.9'da yer almaktadır.

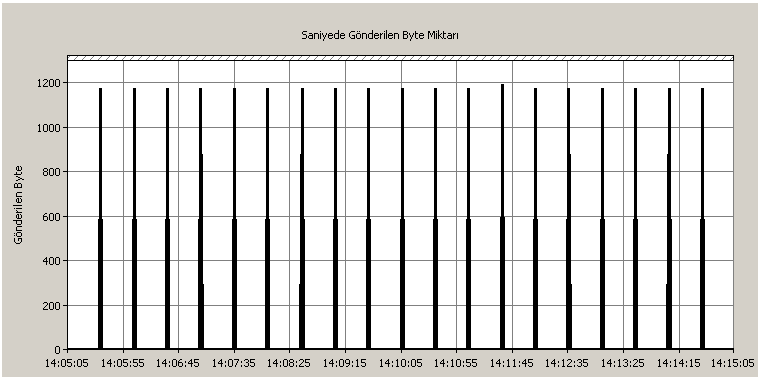
Web sunucusuna yapılan isteklere karşılık gönderilen byte miktarı: Web sunucusuna test süresi içerisinde, gelen isteklere karşılık gönderilen byte miktarı şekil 4.10'da yer almaktadır. Testler sırasında en yüksek değer 1241 byte gözlenmektedir.



Şekil 4.8. Web Sunucu istek cevap süresi – cevap süresi/sn.



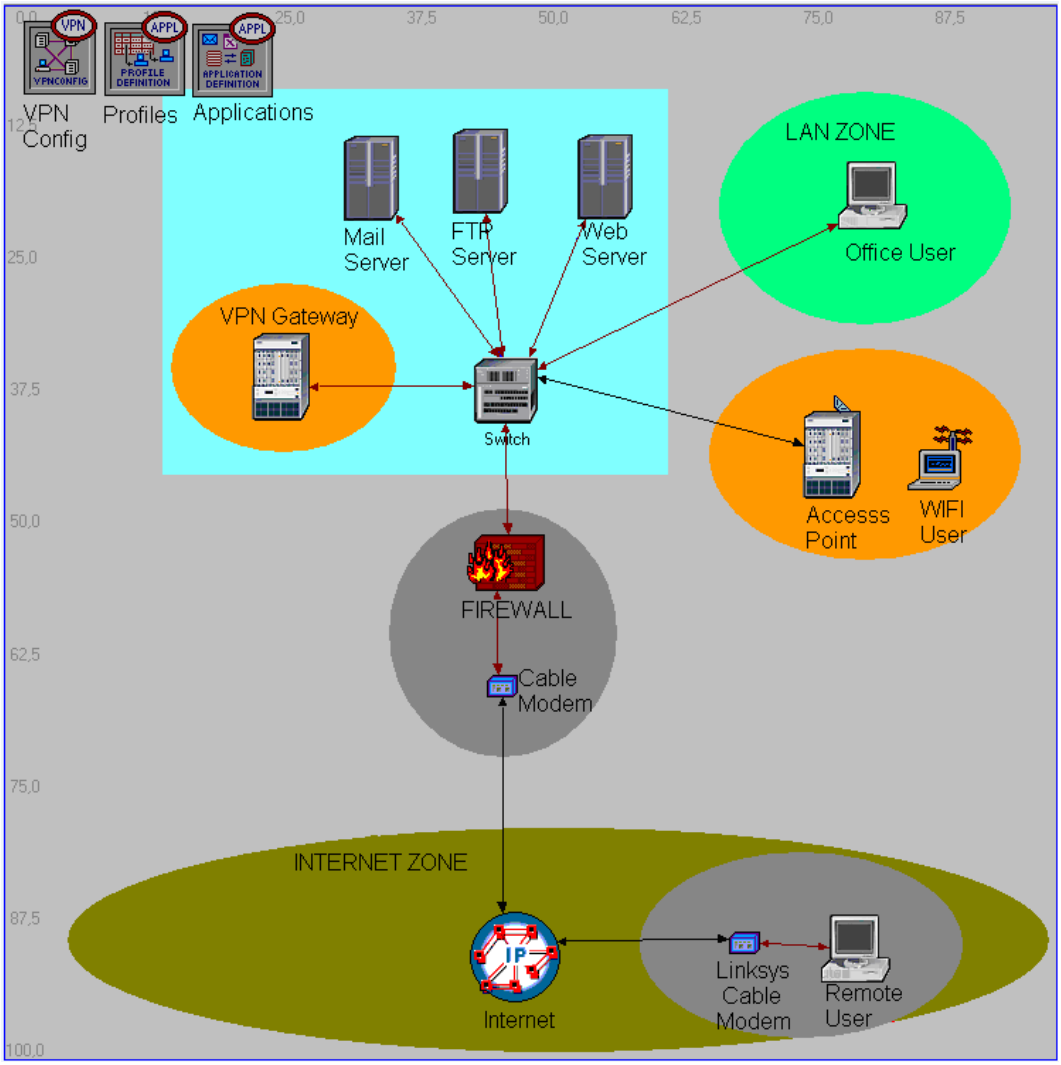
Şekil 4.9. Web Sunucuya gelen istek sayısı– istek/zaman.



Şekil 4.10. Web Sunucudan gönderilen byte miktarı – Gönderilen byte/sn.

4.6. Gerçek Ortamın OPNET ile Modellenmesi

Gerçek ortamda oluşturduğumuz kurumsal ağ modelini, OPNET simülasyon aracı ile inceleyeceğiz. Şekil 4.11'de OPNET ile oluşturulmuş ağ yapısı görülmektedir.



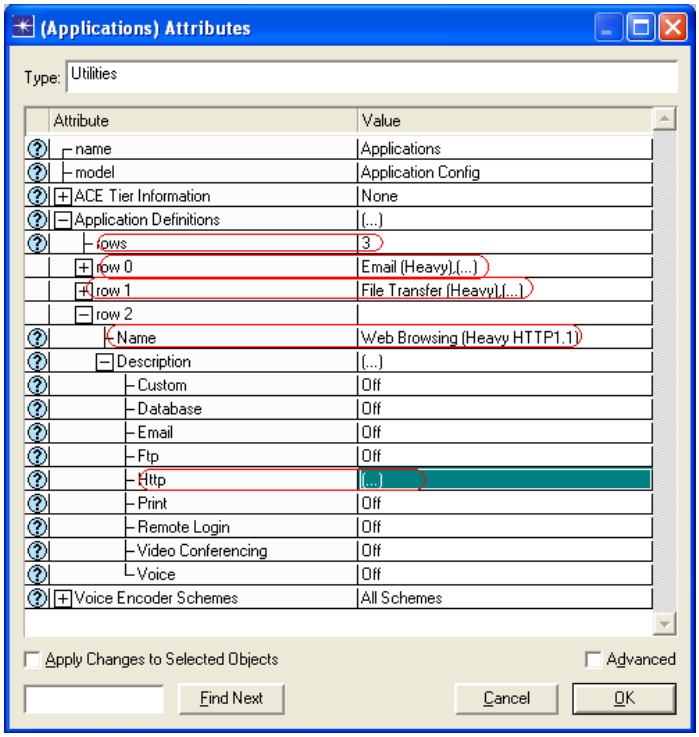
Şekil 4.11. OPNET'te tasarlanan kurumsal ağ modeli.

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. Bu aşamadan sonra yapılacak işlem, sistemde gerçekleştirilecek uygulamaların tanımlanması ve hangi bileşenlerin hangi uygulamalar için kullanılacağının belirlenmesidir.

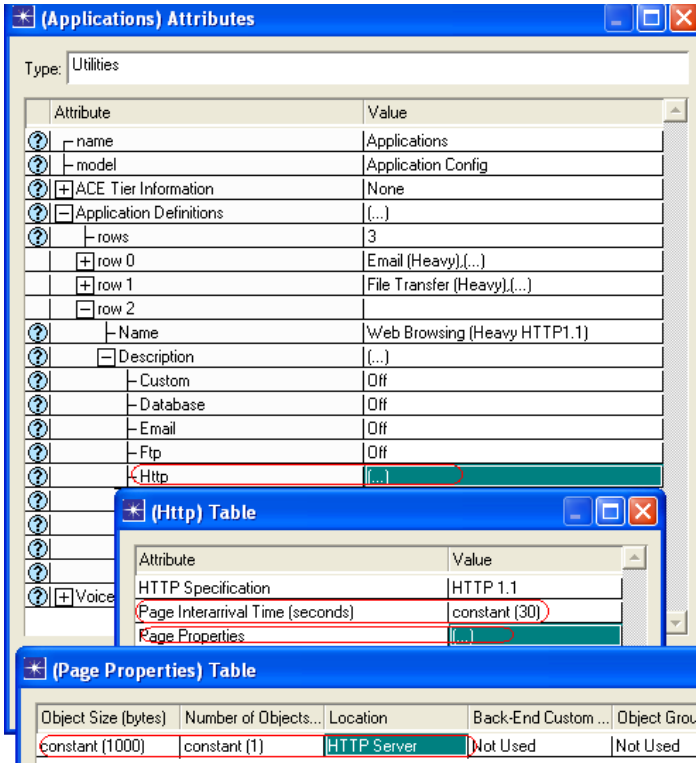
4.6.1. Kurumsal Ağın OPNET Ayarları

Kurum ağında üç farklı sunucu ve 3 farklı kullanıcı bulunmaktadır. Kullanılan sunucular FTP, web ve posta sunucularıdır. Bu özelliklere göre uygulama ve profil ayarları tanımlanmalıdır. Ağda kullanılacak uygulamalar '**Application Config**' nesnesi vasıtasıyla tanımlanmaktadır. Bu üç sunucu uygulamanın her biri için '**Application Config**' üzerinden 'Heavy' özelliği seçilmiştir. Şekil 4.12'de '**Application Config**' nesnesinin ayarları görülmektedir.

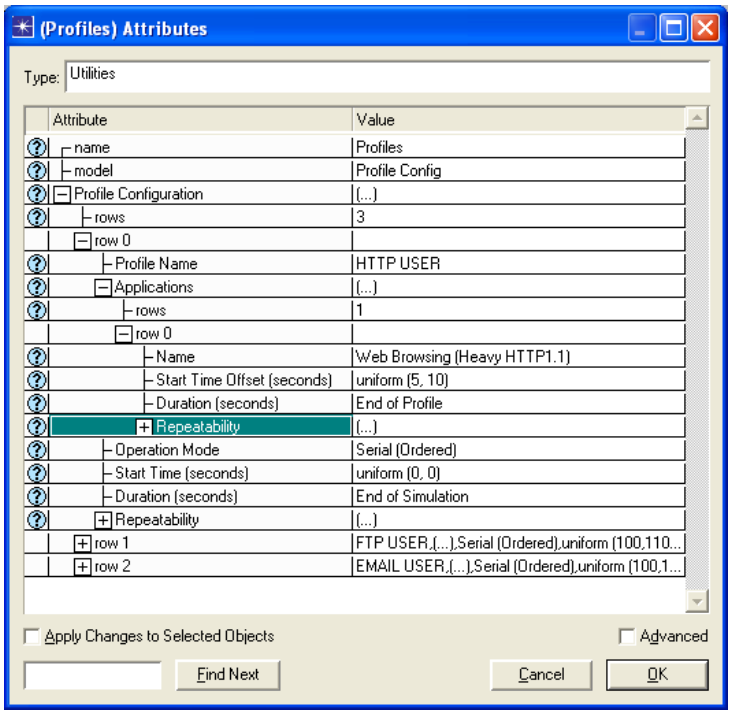


Şekil 4.12. 'Application Config' nesnesi üzerindeki uygulama ayarları.

Simülasyon değerlerinin gerçek ortam ile aynı olması için, '**Application Config**' nesnesi üzerinde 'HTTP Heavy' içersinde yer alan web sayfası büyüklüğü, istek yapılma periyodu ve istek yapılma şeklinin düzenlenmesi gerekmektedir. Şekil 4.13'te web uygulaması ayarları görülmektedir.



Şekil 4.13. 'Application Config' nesnesi üzerindeki web uygulama ayarları.



Şekil 4.14. 'Profile Config' nesnesi üzerindeki ayarları.

"Profiles Config" nesnesini kullanarak, tanımlanan uygulamaların, hangi kullanıcılar tarafından kullanacağının tanımlanmasını yapıyoruz. Bu yapı için 'HTTP USER', 'FTP USER' ve 'EMAIL USER' profilleri oluşturulmuştur. Tanımlamalar şekil 4.14'te görülmektedir.

4.6.2. Kullanıcı Profil Yapıları

Modelde kullandığımız posta sunucusu, web sunucusu ve FTP sunucusu ve Ethernet iş istasyonu (workstation) nesnelerinin tanımları yapılarak nesnelerin yapacakları görevleri belirlemek gerekiyor. Bu nesnelerin sunucular ve kullanıcılar olmak üzere iki farklı ayarı vardır:

I - Kullanıcı Ayarları:

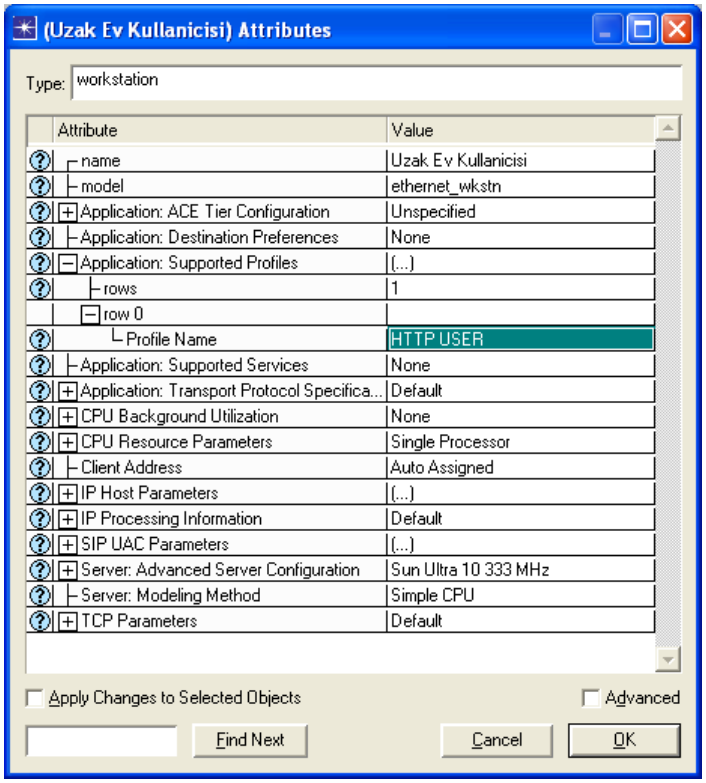
Simülasyon için kullanıcı nesneleri tanımlarıdır. Bu nesneler, daha önce tanımladığımız "**Profiles Config**" içersindeki 'HTTP USER', 'FTP USER' ve 'EMAIL USER' profillerinden hangilerinin kullanılacağı tanımı yapılır. Kullanıcı profillerinin eriştiği uygulamalar Tablo 4.1'de, nesnelerinin yapılanışı ise Şekil 4.15'da verilmiştir.

Tablo 4.1. Kullanıcı profillerinin kullandığı uygulamalar.

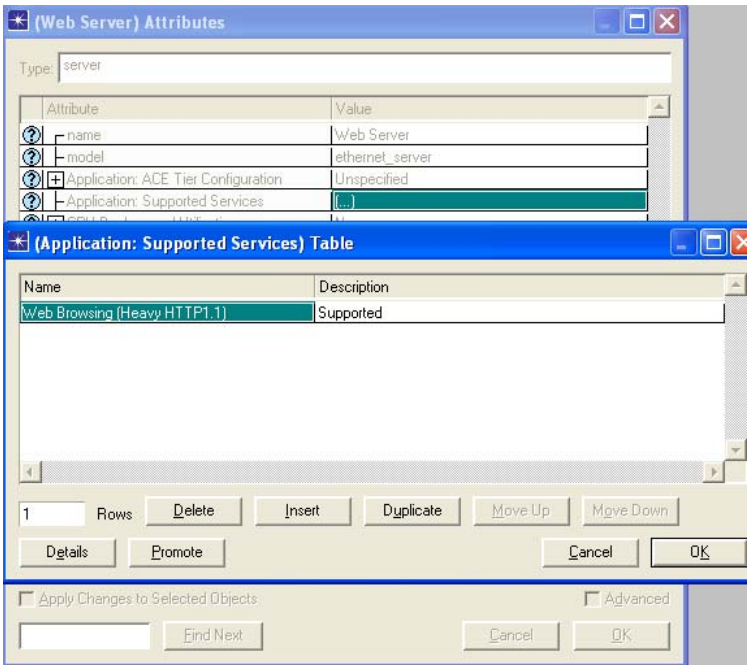
Profile Adı	**Kullandığı Uygulamalar**
HTTP USER	'Web Browsing'
EMAIL USER	'Email'
FTP USER	'File Transfer'

II - Sunucu Ayarları:

Senaryomuzda üç adet 'Ethernet_server' nesnesi kullanıyoruz. Bu nesnelerden hangisinin, hangi uygulama için servis vereceği ayarının yapılması gerekir. Projemizdeki ethernet_server nesneleri Şekil 4.16'da olduğu gibi hizmet vereceği sunucu ismi verilerek nesne ismi değiştirilir, ethernet_server nesnesinin 'Applicator Suported Server' değerine hizmet vereceği servis veya servisler atanarak düzenlemeleri yapılır.



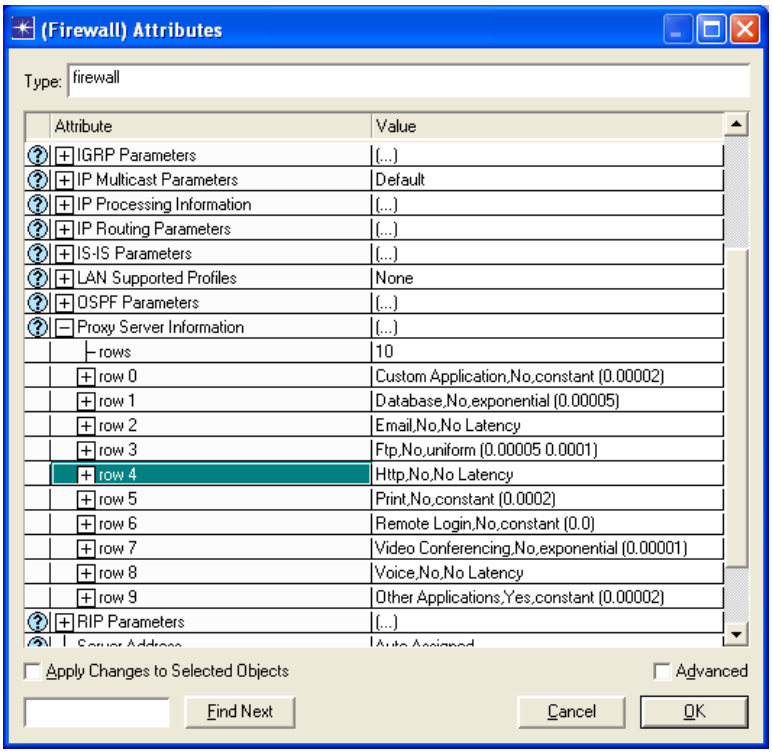
Şekil 4.15. 'ethernet_wkstn' nesnesinin ayarları.



Şekil 4.16. 'Ethernet_server' nesnesine servis atanması.

4.6.3. Güvenlik Duvarı Nesnesinin Yapılanışı

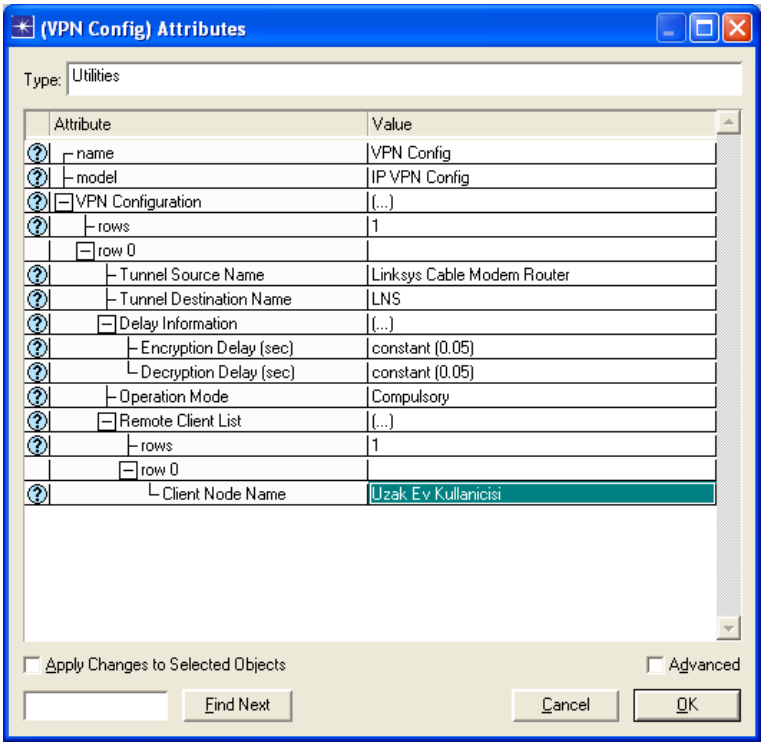
Güvenlik Duvarı nesnesi üzerinden FTP sunucusu, Web sunucusu ve E-mail sunucu erişimlerini engelledik. Böylelikle kurum dışından kurum iç ağa erişim engellenmiş oldu. Şekil 4.17'de Güvenlik Duvarı nesnesinin özellikleri ve uygulanan kurallar yer almaktadır. Güvenlik Duvarı'nın 'Proxy Server Information' özelliği altındaki 'rows' tanımları ile uygulamların kuralları belirlenir.



Şekil 4.17. Güvenlik duvarı üzerinde uygulanan kurallar.

4.6.4. 'VPN Config' Nesnesinin Yapılanışı ve VPN Ayarları

Kurum ağının güvenlik duvarı ayarlandıktan sonra kurum dışından hiçbir şekilde Kurum Yerel Ağı'na erişim mümkün olmamaktadır. Kurumun uzak çalışanlarının kurum kaynaklarına erişimi için simülasyonumuzda '**Internet Tool Box**' paletinde yer alan 'VPN Config' nesnesini kullanıyoruz. Bu nesne ile bir veya birden fazla yönlendirici arasında VPN tanımı yapılabiliyor. Şekil 4.18'de '**VPN Config**' nesnesinin yapılanışı yer almaktadır.

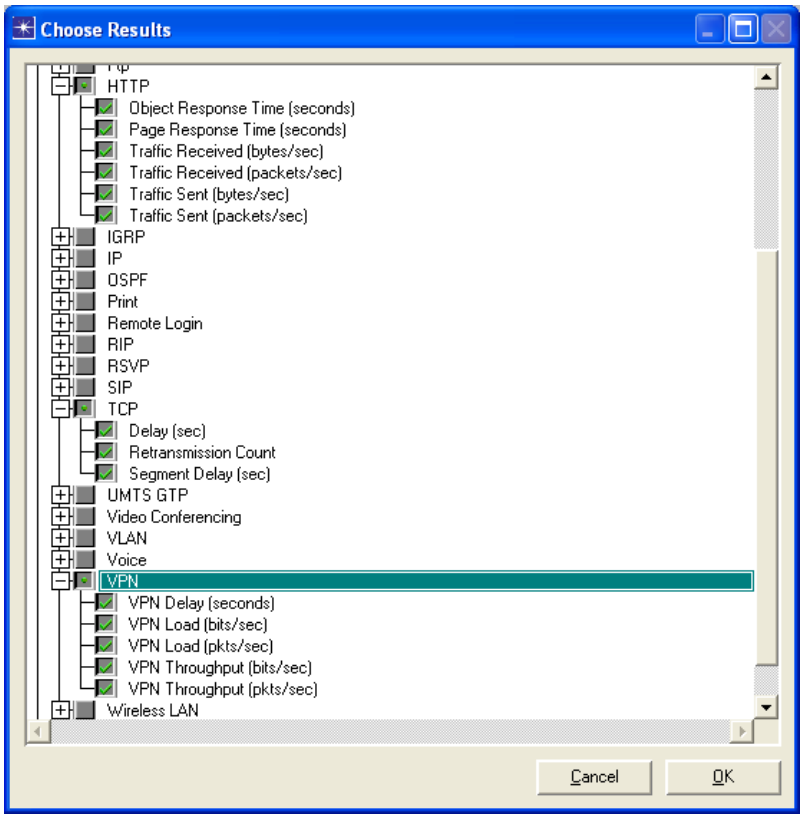


Şekil 4.18. 'VPN Config' nesnesinin ayarları.

Senaryodaki iki cihazın VPN tüneli oluşturabilmeleri için '**VPN Config**' nesnesinin '**VPN Configuration**' özelliğinin '**rows**' değeri 1 yapılır ve açılan '**row 0**' alanında VPN yapacak yönlendiriciler, kaynak ve hedef alanına tanımlanır. Bu işlem ile yönlendiriciler arasında VPN tanımı yapılmış olur, fakat yönlendiriciye bağlı kullanıcıların kuruma erişebilmeleri için '**Client Node Name**' alanına erişim yapacak kullanıcıların girilmesi gerekmektedir.

4.7. Analizler ve Sonuçlarının Karşılaştırılması

Ayarlarımızı tamamladıktan sonra, oluşturduğumuz senaryolarda simülasyon sonuçlarını karşılaştırabilmemiz için hangi verilerin toplanması gerektiğine karar verilmesi gerekiyor. Gerçek ortamda Web sunucusu üzerinde testler yaptığımız için HTTP ve IP verilerini hesaplayacağız. Şekil 4.19'da toplanmasını istediğimiz **Global Statics** verileri yer almaktadır.



Şekil 4.19. Simülasyon sırasında toplanacak değerler.

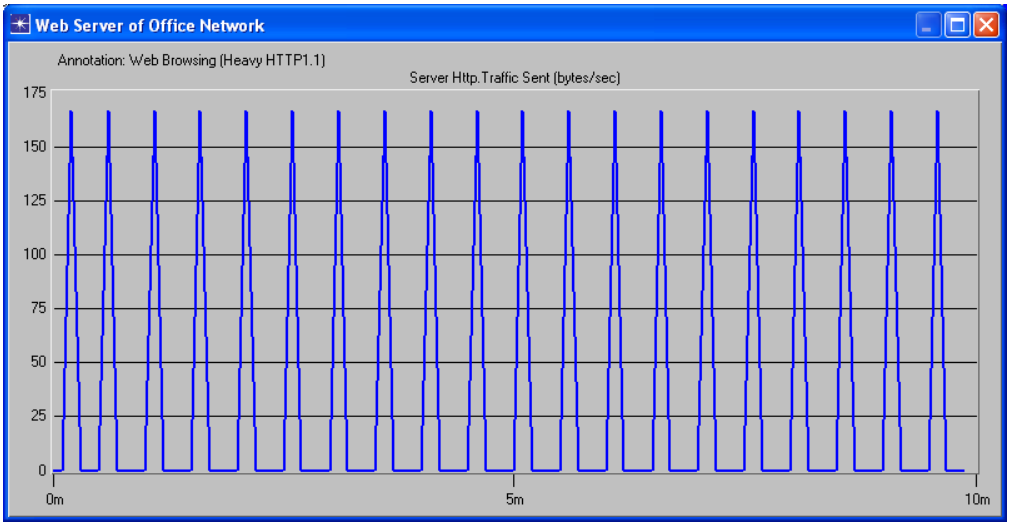
Simülasyonun çalışması bittikten sonra aşağıdaki rapor bilgisi oluşmuştur:

```
Beginning simulation at 17:56:58 Paz Tem 18 2010
Simulation Completed - Collating Results.
Events: Total (34125), Average Speed (18989 events/sec.)
Time: Elapsed (2 sec.), Simulated (10 min. 0 sec.)
Simulation Log: 8 entries
```

Senaryonun çalışma süresi 2 saniye ve gerçekleşen toplam olay sayısı 34.125'tir.

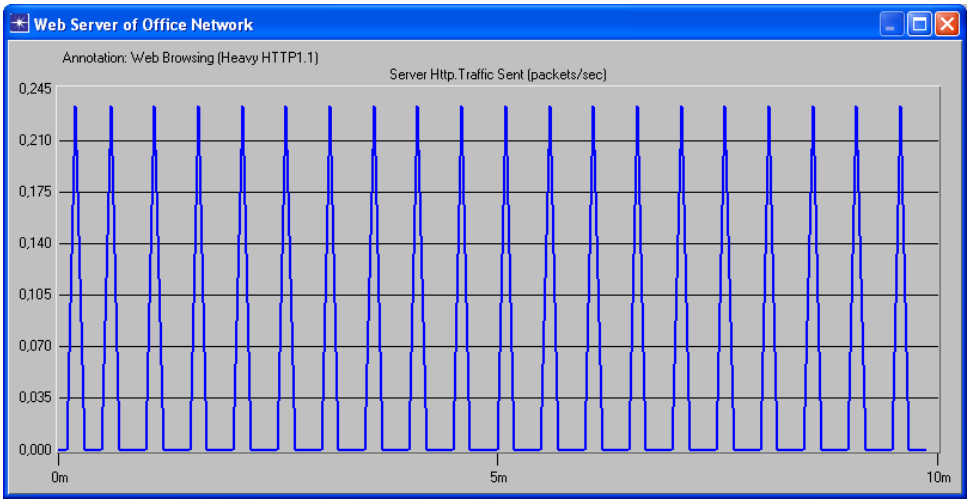
4.7.1. HTTP Sunucusu Simülasyon Grafikleri

VPN bağlantısı ile kurum ağına bağlanan Uzak Ev Kullanıcısının Güvenlik Duvarı üzerinden web sunucusuna erişim simülasyonunda Web Sunucusunun cevap verdiği byte büyüklükleri Şekil 4.20'de yer almaktadır. Simülasyon sonucuna göre web sunucusu, 30 sn'de bir istek yapan kullanıcıya, 170 byte büyüklüğünde HTTP cevapları dönmektedir.



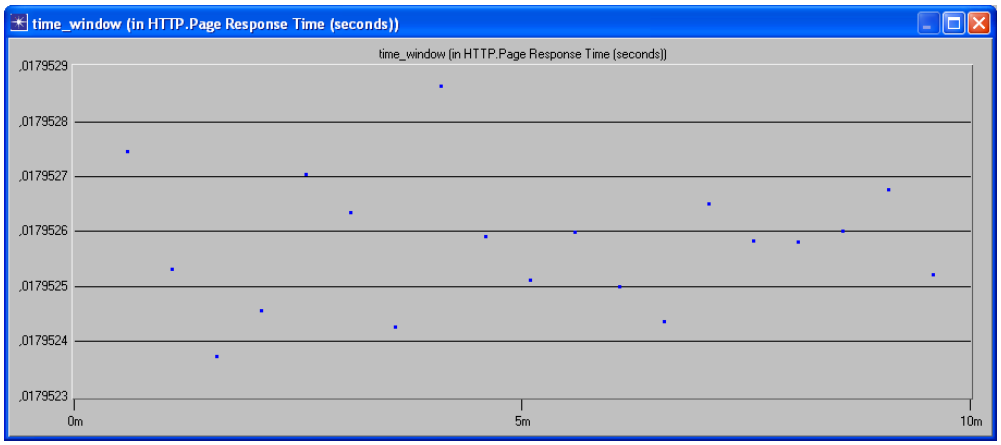
Şekil 4.20. 'HTTP Traffic Sent' grafiği – byte/sn.

Web sunucusuna gelen isteklere dönülen paketlerin grafiği Şekil 4.21'de yer almaktadır. Simülasyon sonucuna göre isteklere dönülen paket büyüklükleri 0.220 paket/sn seviyelerindedir.



Şekil 4.21. 'HTTP Traffic Sent' grafiği – paket/sn.

Web sunucusunun isteklere yanıt verme süresinin grafiği Şekil 4.22'de yer almaktadır. Simülasyon sonucuna göre, isteklere yanıt verme süreleri 0,179 ms'dir.

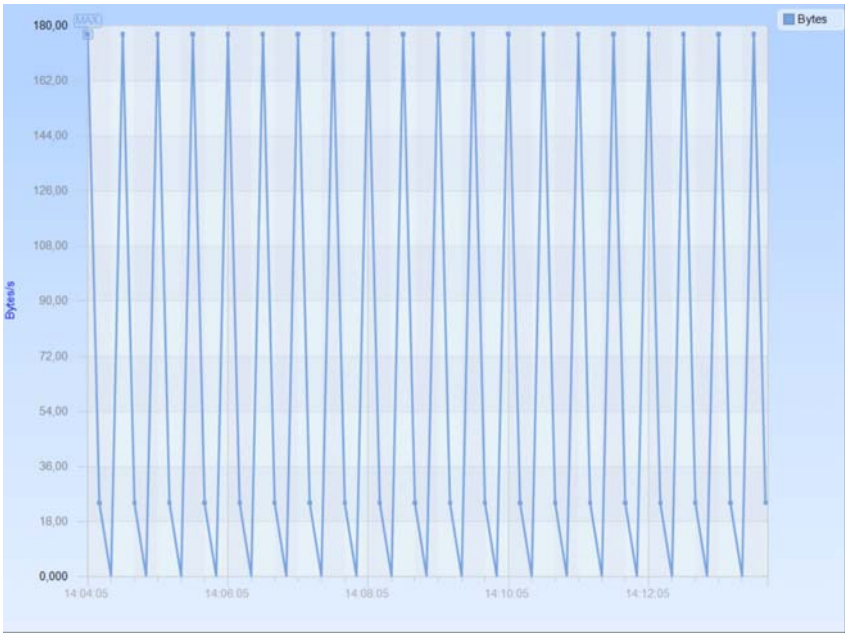


Şekil 4.22. 'HTTP Response Time' grafiği – cevap süresi/sn.

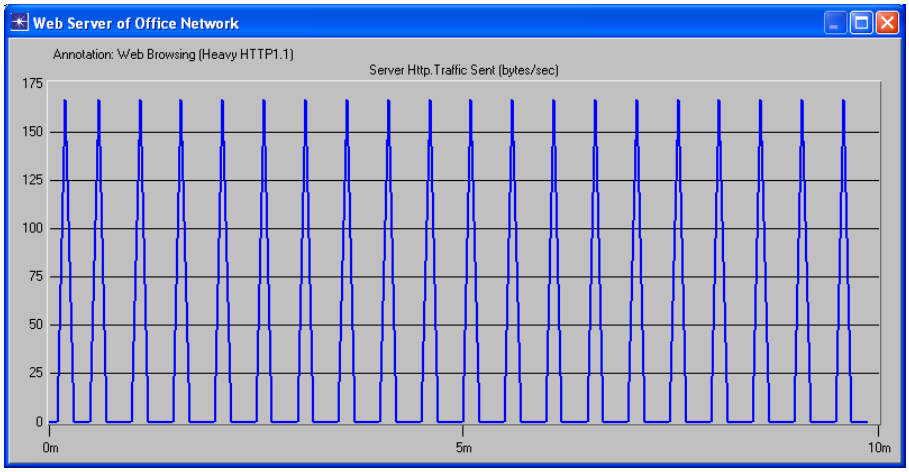
4.8. Gerçek Ortamın Test Sonuçları ile OPNET Simülasyon Sonuçlarının Karşılaştırılması

4.8.1. Web Sunucusundan Saniyede Gönderilen Veri Miktarı

Gerçek ortamda yapılan testlerde CACE Pilot uygulaması ile yapılan analizlerde Web sunucusunun yanıt verdiği veri büyüklüğü Şekil 4.23'ten de görülebileceği gibi 175 byte olarak gözlenmiştir. OPNET ortamında yapılan analizde de Şekil 4.25'tende görülebileceği gibi "**HTTP Trafik Sent**" grafiğinde gözlemlenen veri büyüklüğü 170 byte'tır. Bu sonuçlar göz önünde tutulduğunda her iki grafikteki değerlerin birbirine yakın olduğu ve simülasyon ortamındaki değerler ile gerçek ortamdaki değerlerin birbirini doğruladığı gözlemlenmektedir.



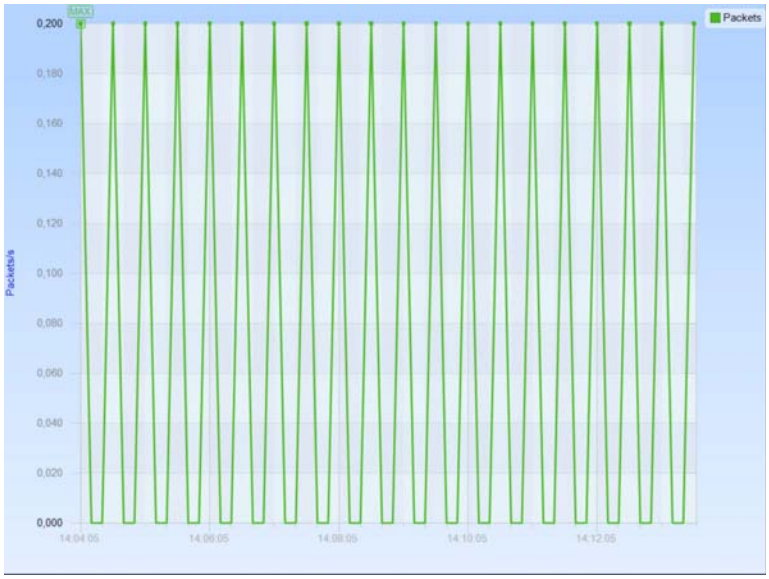
Şekil 4.23. Gerçek ortan kullanılan bant genişliği – byte/sn.



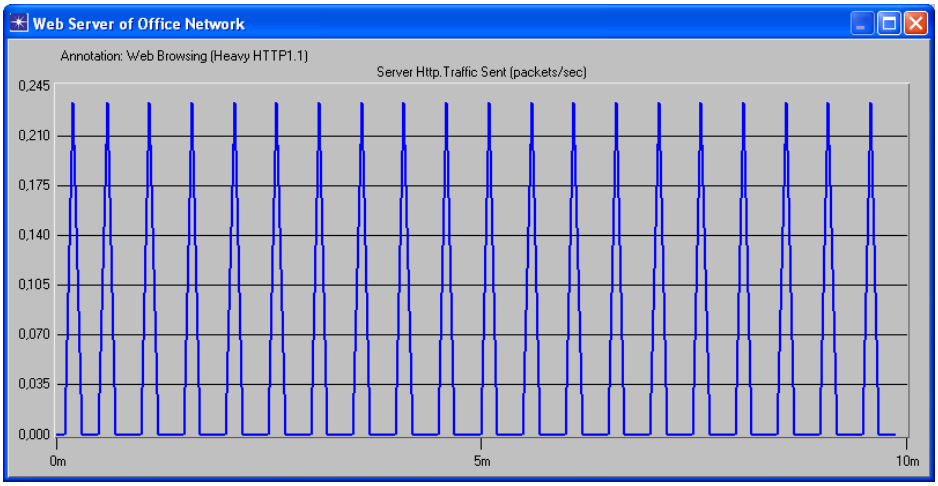
Şekil 4.25. Sanal ortam 'HTTP Traffic Sent' grafiği – byte/sn.

4.8.2. Web Sunucusundan Saniyede Gönderilen Paket Miktarı

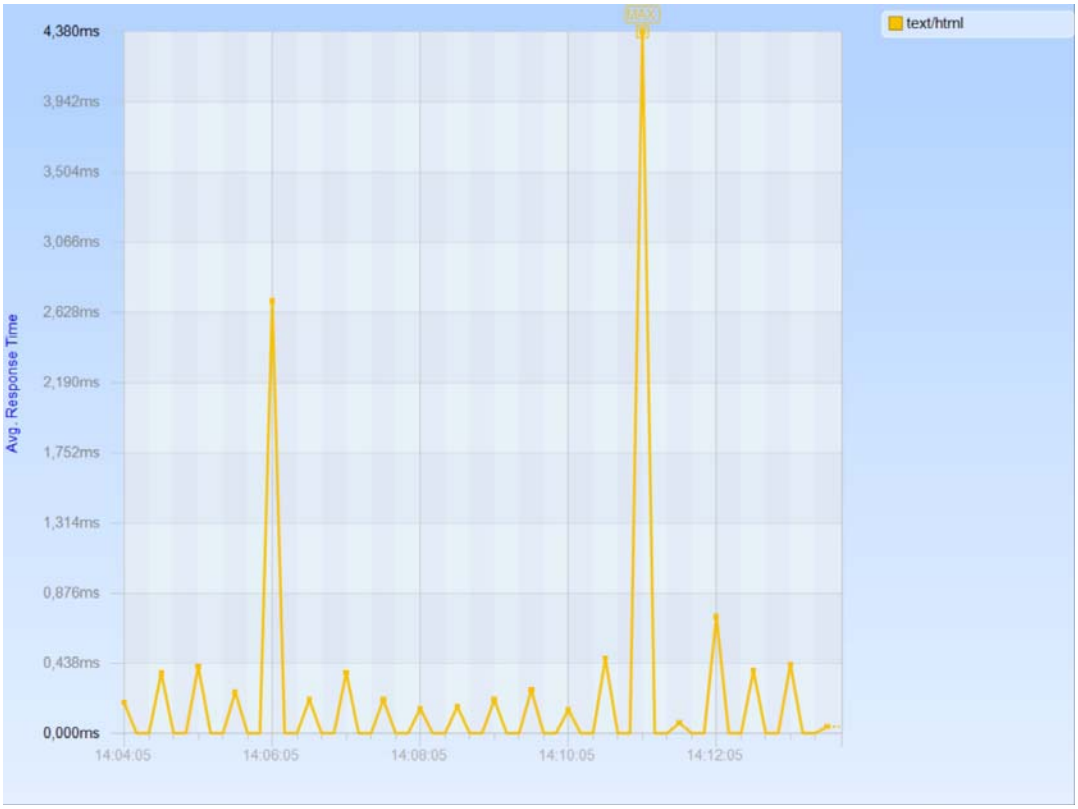
Gerçek ortamda CACE Pilot uygulaması ile yapılan analizlerde saniyede gönderilen paket grafiği Şekil 4.26'da görülmektedir. Grafiğe göre saniyede gönderilen paket miktarı 0,200 olarak gözlenmektedir. OPNET simülasyon ortamında yapılan simülasyon analizinin grafiği de Şekil 4.27'de yer almaktadır. Simülasyon analizinde saniyede gönderilen paket miktarı 0.220 olarak görülmektedir. Bu iki grafiği karşılaştırdığımızda saniyede gönderilen veri miktarında olduğu gibi birlerine yakın ve benzer sonuçlar verdiği elde edildi.



Şekil 4.26. CACE Pilot analizleri sonucunda oluşan kullanılan bant genişliği – paket/sn.



Şekil 4.27. OPNET simülasyonları sonucu oluşan 'HTTP Traffic Sent' grafiği – paket/sn.

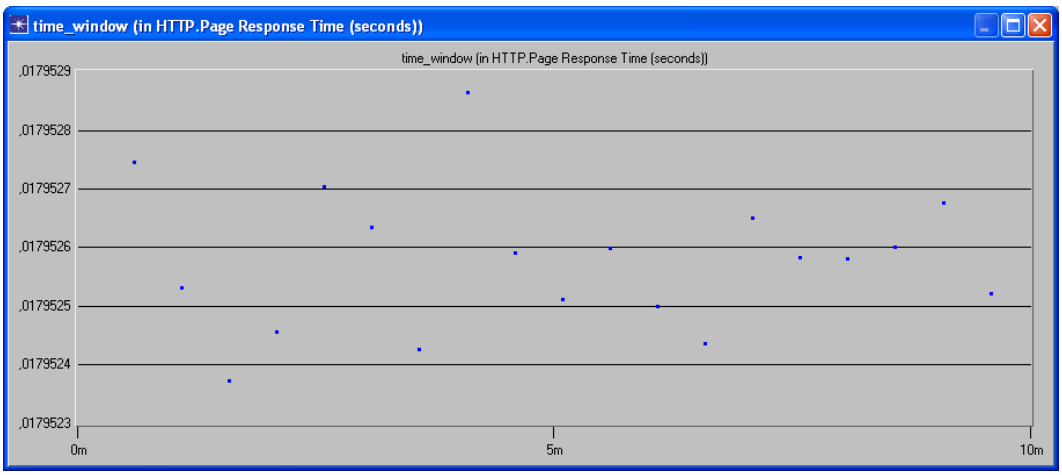


Şekil 4.28. Gerçek ortam web sunucusu istek yanıt süreleri – yanıt süresi/sn.

4.8.3. Web Sunucusunun Cevap Süreleri

Gerçek ortamda CACE Pilot uygulaması ile yapılan analizlerde yapılan HTTP isteklerine verilen cevapları süreleri Şekil 4.28'da görülmektedir. Grafiğe göre cevap süreleri Internet ortamının kararlı olmamasından dolayı değişken bir grafiğe sahiptir. İstek-cevap süreleri

ortalama 0.2 sn olarak gözlenmektedir. OPNET simülasyon ortamında ise Şekil 4.29'de de görülebileceği gibi istek cevap süreleri birbirlerine yakın değerler olup ortalama 0.18 sn değerindedir. Gerçek ortamda Internet ağ trafiğinde anlık değişmelerin olmasından dolayı oluşan yüksek yanıt sürelerini göz ardı edersek, gerçek ortam ile simülasyon ortamının birbirini çok yakın sonuçlar verdiğini görmekteyiz.



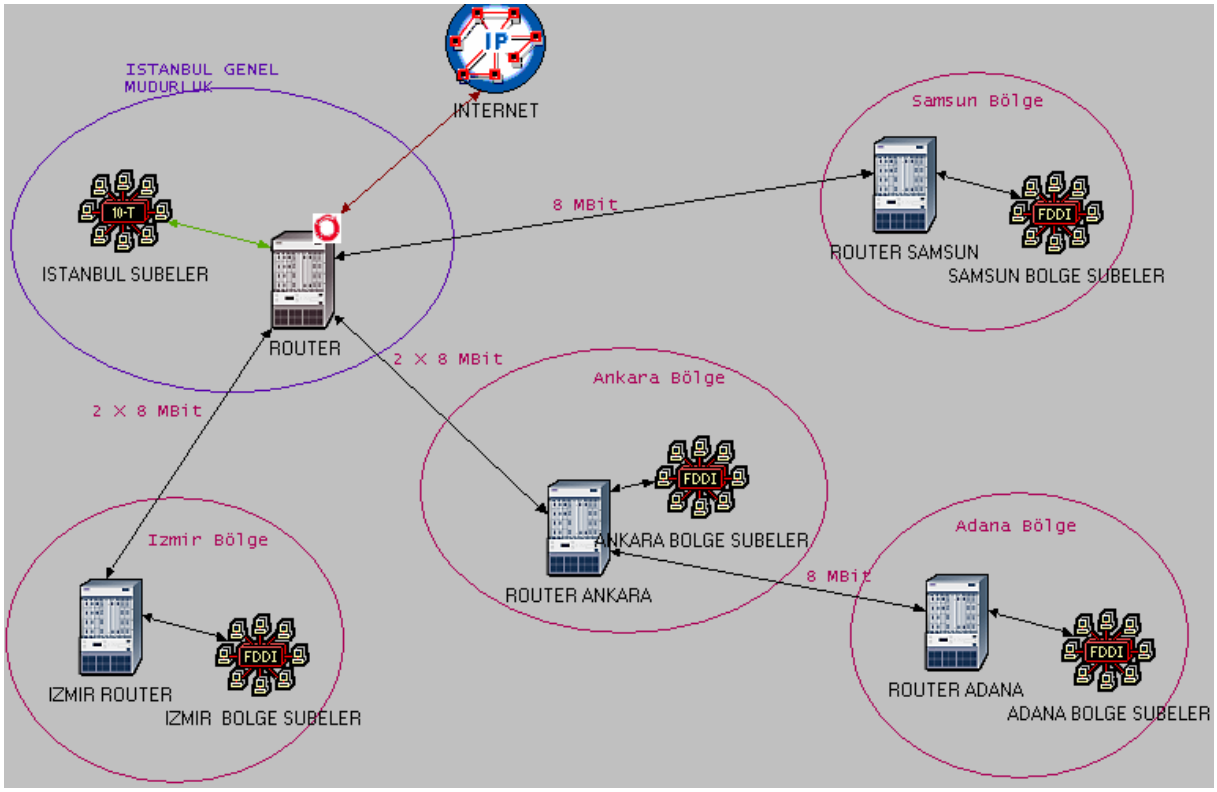
Şekil 4.29. OPNET simülasyon ortamı 'HTTP Response Time' grafiği – yanıt süresi/sn.

Sonuç olarak, gerçek ortamda yapılan testler ile OPNET ortamında yaptığımız simülasyonlar sonucunda, gerçek ortam ile simülasyon ortamındaki sonuçların birbirlerine yakın olduğunu ve her iki ortamdaki sonuçların birbirlerini desteklediğini söyleyebiliriz. Bu sonuçlar doğrultusunda, OPNET ile yapılacak modellemelerin ve analizlerin doğruluğuna güvenilebilir, daha büyük yapılardaki kurumsal ağ yapıları tasarlanarak simülasyonlar yapılabilir sonucuna varılmıştır.

5. DAHA GERÇEKÇİ BİR KURUMSAL AĞ MODELİ

5.1.1. Kurumsal Ağın Tasarlanması ve Kurumsal Ağın Genel Görünümü

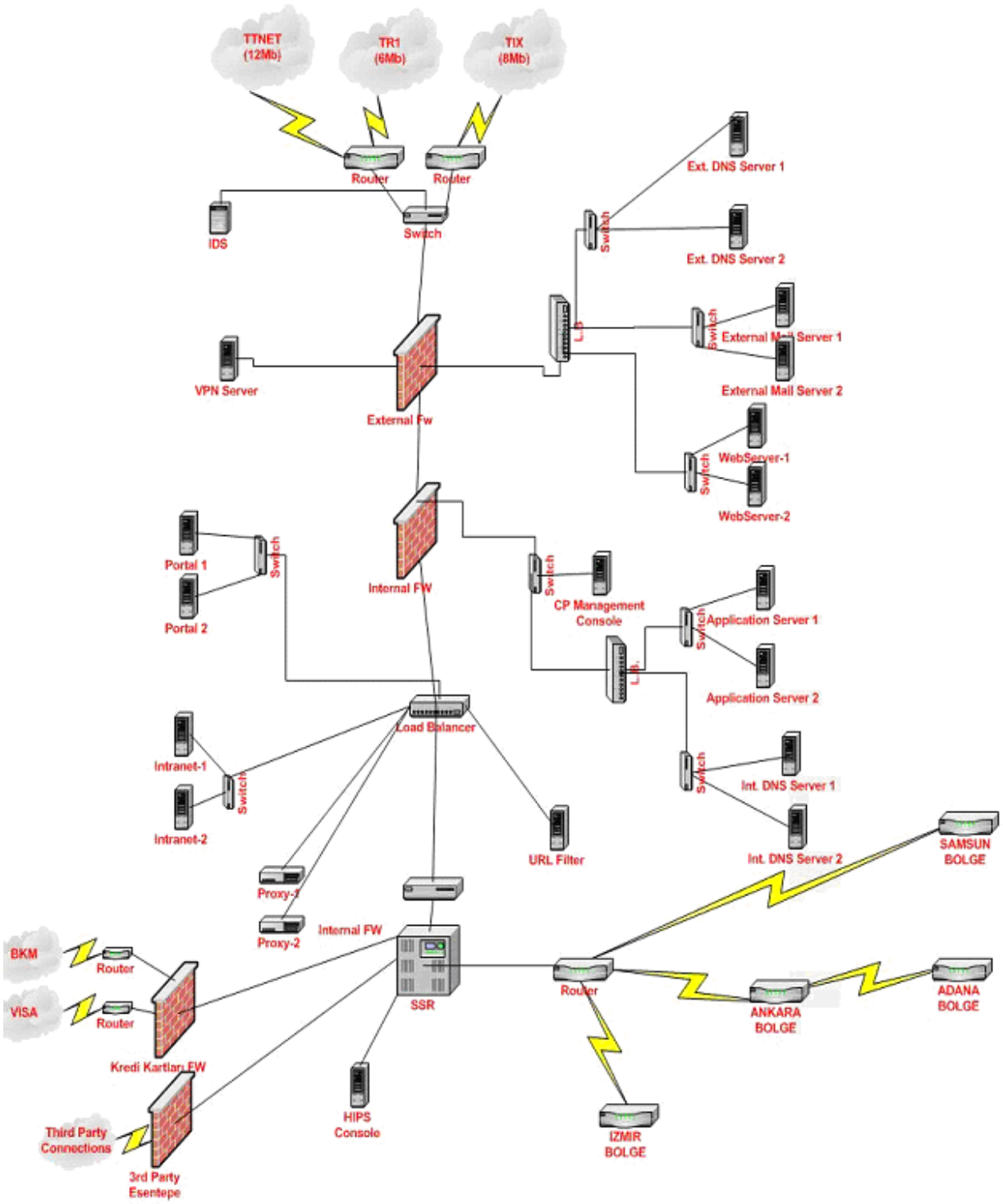
Tezimizde daha gerçekçi bir kurum ağı tasarımı için, 3000 çalışanı ve 80 tane şubesi ile Türkiye'nin birçok noktasında finansal hizmet veren tipik bir örnek verilmiştir. Kurum, genel müdürlüğün bulunduğu İstanbul ile birlikte beş bölgeden oluşmakta ve bölgelerin her birinde bir şube, bölgenin merkez şubesi olarak tanımlanmaktadır. İzmir ve Ankara 2 X 8 Mbit, diğer şubeler 8 Mbit kiralık hat (leased line) ile genel müdürlüğe bağlanmaktadır. Bölgelerdeki diğer şubeler, genel müdürlüğe erişimlerini bağlı oldukları merkez şube üzerinden gerçekleştirirler. Şekil 5.1'de tasarlanan kurumsal ağın genel yapısı yer almaktadır.



Şekil 5.1. Tasarlanan kurumsal ağın genel yapısı.

5.1.2. Kurumsal Ağın Bilgi İşlem Altyapısı

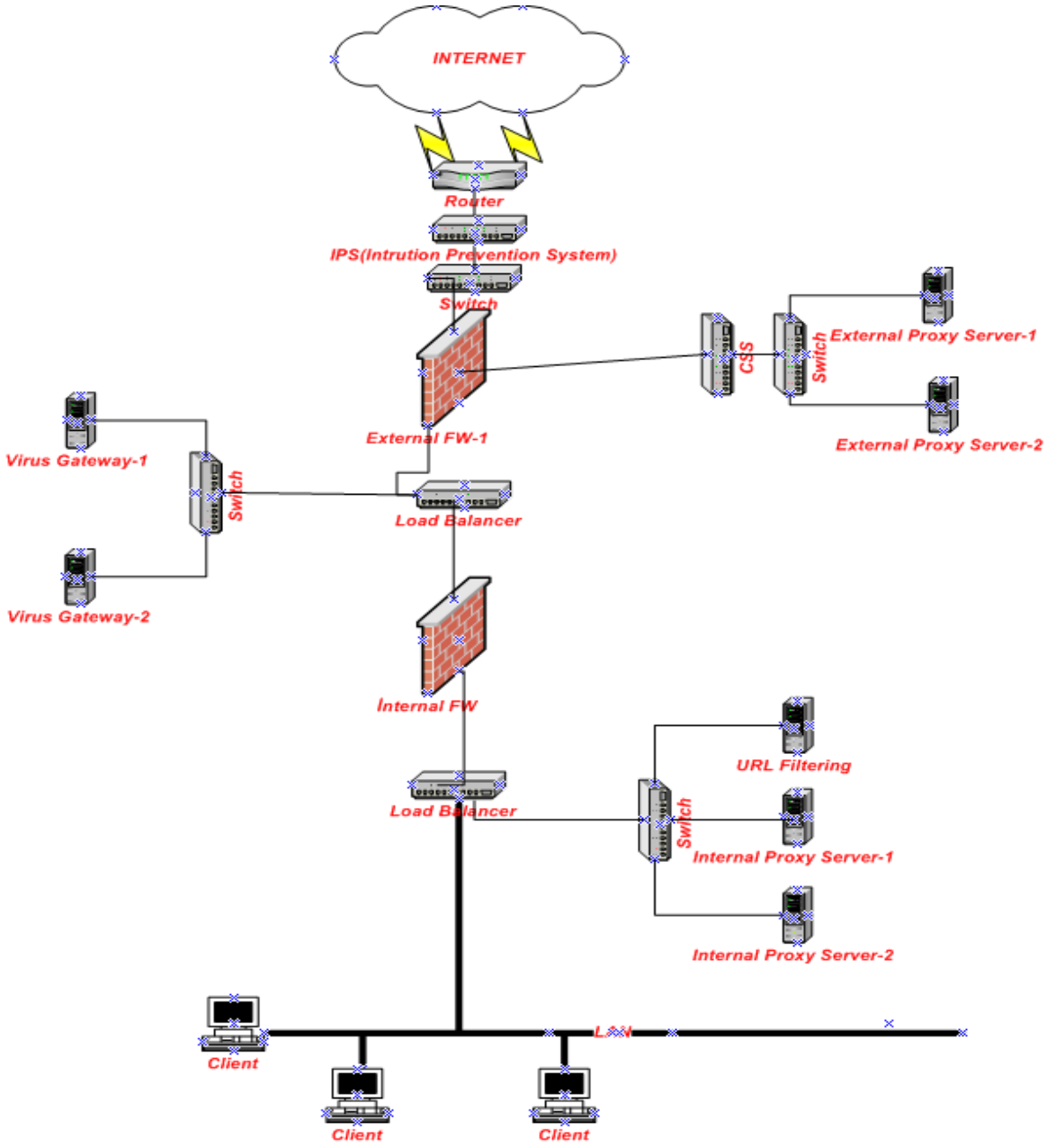
Tasarladığımız kurumsal ağın, güveliğini sağlamak için alt yapısında Güvenlik Duvarı, IDS, HIPS (Host-based Intrusion Prevention System / Bilgisayar-tabanlı Atak Önleme Sistemi) ve URL Filter kullanmaktadır. Şekil 5.2'de bu kurumsal ağın diyagramı yer almaktadır.



Şekil 5.2. Tasarlanan kurumsal ağın diyagramı.

5.1.3. Kurum İnternet Erişimi

Kurumun tüm kullanıcıları İnternet erişimini genel müdürlük üzerinden gerçekleştirir. Kurum Internet erişim ağ diyagramı şekil 5.3'te yer almaktadır.

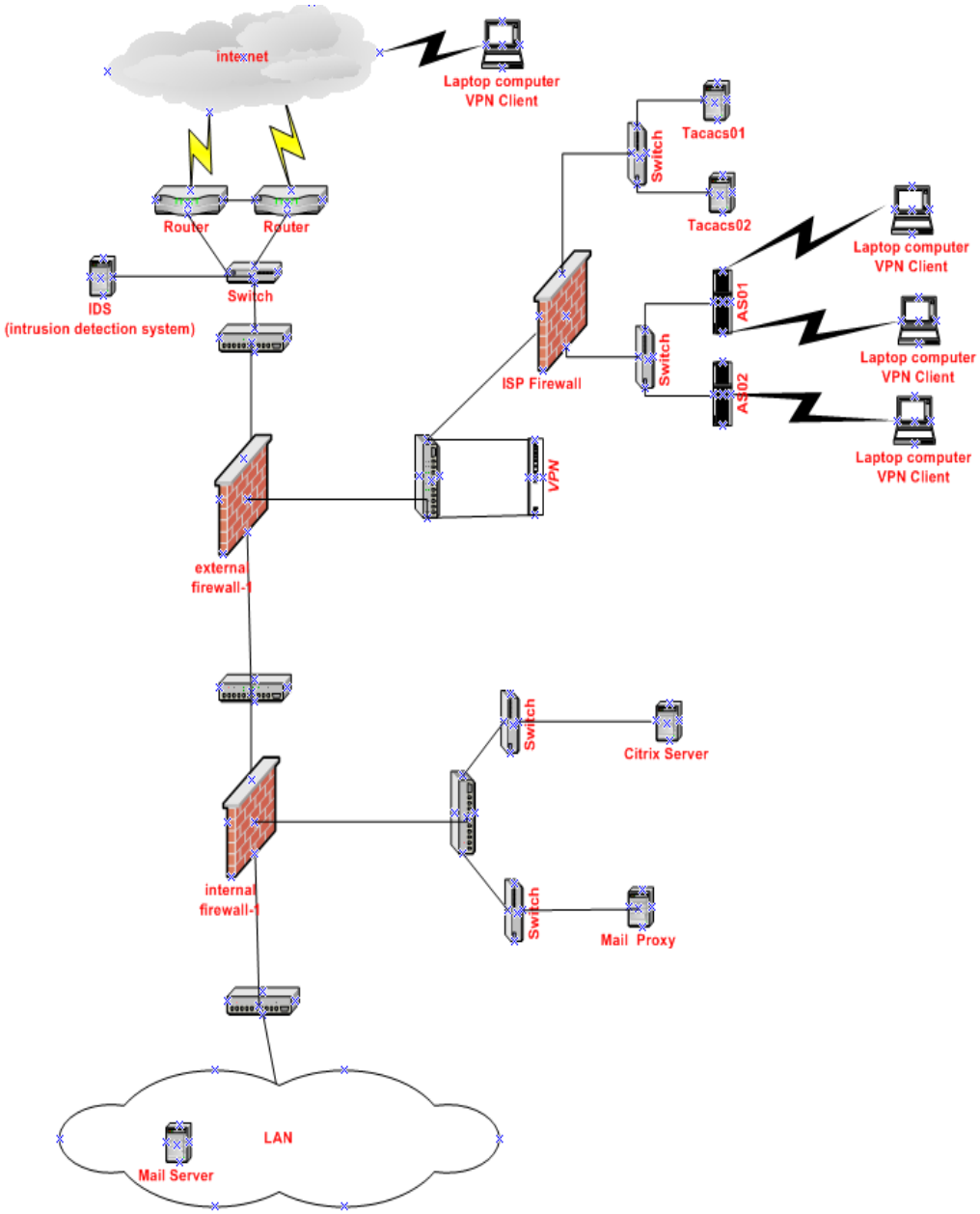


Şekil 5.3. Kurum internet erişim diyagramı.

Kurum çalışanlarından biri, İnternet sayfası isteği yaptığında, bu istek ilk olarak Internal Proxy'e gider. Internal Proxy bu isteği URL Filter'a yönlendirir. URL Filter'da istek uygun görülür ise, External Proxy'e yönlendirilerek, talep edilen İnternet sayfasının bulunduğu sunucuya yönlendirilir. External Proxy'e gelen cevap Virus Gateway'a yönlendirilir. Gelen cevapta bir risk gözlenmez ise Internet Proxy ile talebi yapan kullanıcıya cevap dönülmüş olur.

5.1.4. Kurum VPN Bağlantısı

Kurum personellerinden yetkisi olan kullanıcılar, kurum dışından kurum sistemlerine erişim için Şekil 5.4'teki VPN alt yapısını kullanır. Kurum dışından bir kullanıcı kuruma erişmek için, sahip olduğu token ile bilgisayarındaki VPN istemcisini kullanarak VPN sunucusuna gelir ve kimlik doğrulaması yapar. Kimlik doğrulaması başarıyla gerçekleştikten sonra kullanıcı VPN'den bir IP alarak sisteme dahil olur. Kullanmakta olduğu bilgisayardaki Citrix istemcisi ile VPN üzerinden Citrix sunucusuna bağlanır ve kurum kaynaklarına erişim sağlamış olur.



Şekil 5.4. Kurum VPN altyapısı.

6. OPNET İLE BİR KURUMSAL AĞIN MODELLENMESİ VE ANALİZİ

6.1. Giriş

Bu bölümde; önceki bölümde tasarlanan kurumsal ağ yapısının, Güvenlik Duvarı (Firewall) ve VPN güvenlik yapılarının OPNET simülasyon programının gerçekleştirebildiği yapı çerçevesinde simülasyonu yapılarak, ağın performansına etkileri karşılaştırılmakta, tez çalışmasının diğer önemli kısmını oluşturan Kurumsal Ağların Güvenliği ile ilgili simülasyonlar gerçekleştirilmektedir.

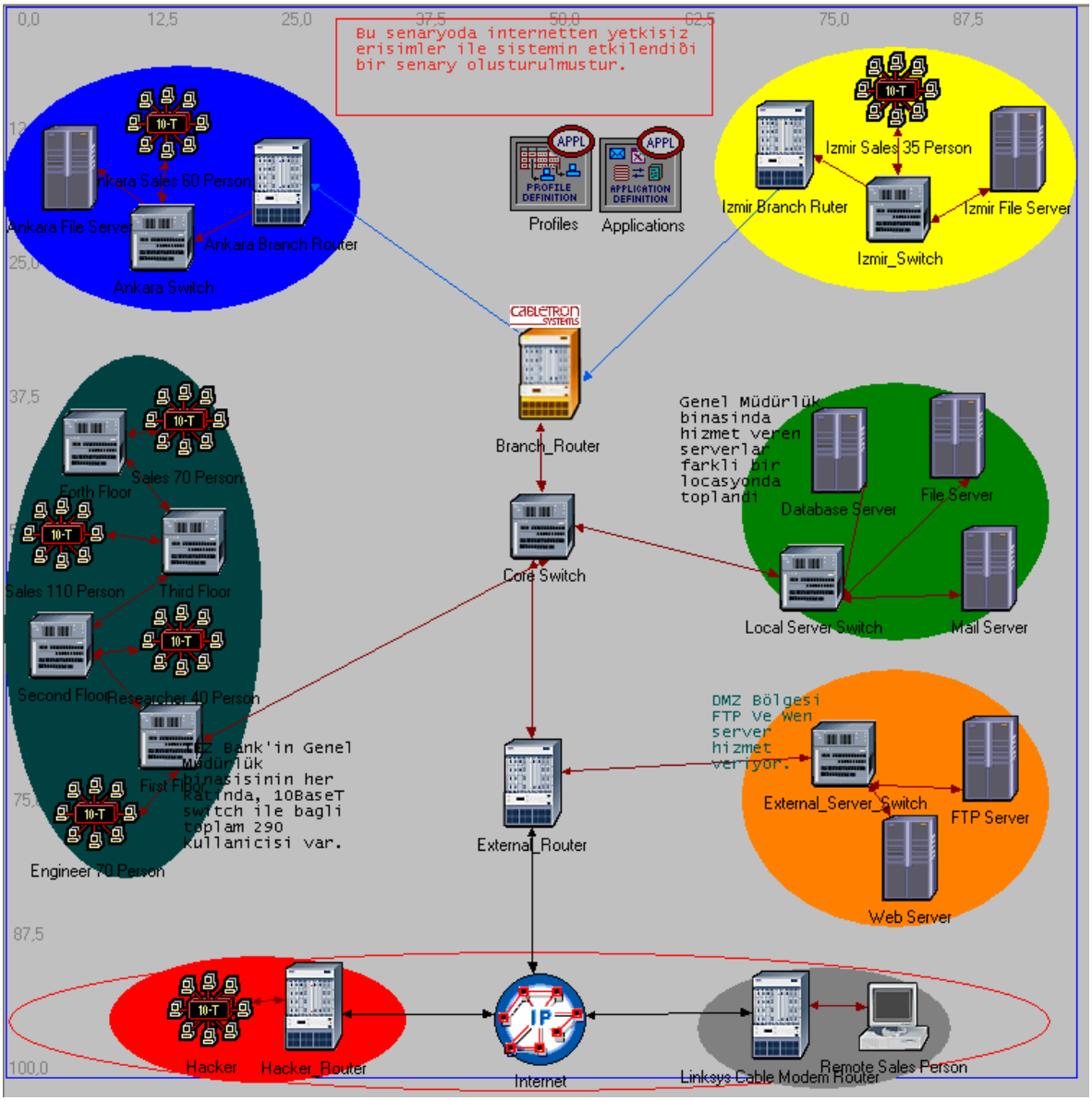
6.2. Güvenlik Duvarı ve VPN Kullanımı ile Yetkisiz Erişimlerin Sisteme Etkisinin İncelenmesi

OPNET ile tasarladığımız bir kurum ağında Güvenlik Duvarı ve VPN kullanımının sisteme etkilerini inceleyeceğiz. Oluşturduğumuz 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. Oluşturduğumuz kurumun yapısını iki farklı senaryo ile analiz edeceğiz.

6.3. Güvenlik Duvarı ve VPN Kullanılmadan (Firewall_VPN_NO) Oluşturulan Kurum Ağı

Birinci senaryomuz olan Güvenlik Duvarı ve VPN kullanmadığımız yapıda, kurum dışından ve kurum içinden tüm kullanıcılar mevcut yapıdaki her noktaya erişim sağlayabilmektedir. Şekil 6.1'de OPNET'te oluşturduğumuz yapının ağ şeması yer almaktadır.

Senaryomuzda; dış (external) bölge diye nitelendirdiğimiz alanda web ve dosya aktarım sunucusu, yerel sunucu bölgesi şeklinde tanımladığımız alanda da posta sunucusu, veritabanı sunucusu ve dosya sunucusu olmak üzere beş sunucunun bulunduğu bir kurum ile, Engineer, Researcher, E-Commerce Customer, Sales Person, Multimedia User, Hacker Group adlı kullanıcıların bulunduğu kurum içi ve dışından gelen trafik incelenmiştir.



Şekil 6.1. Güvenlik duvarı ve VPN kullanılmadan oluşturulan kurum ağı şeması.

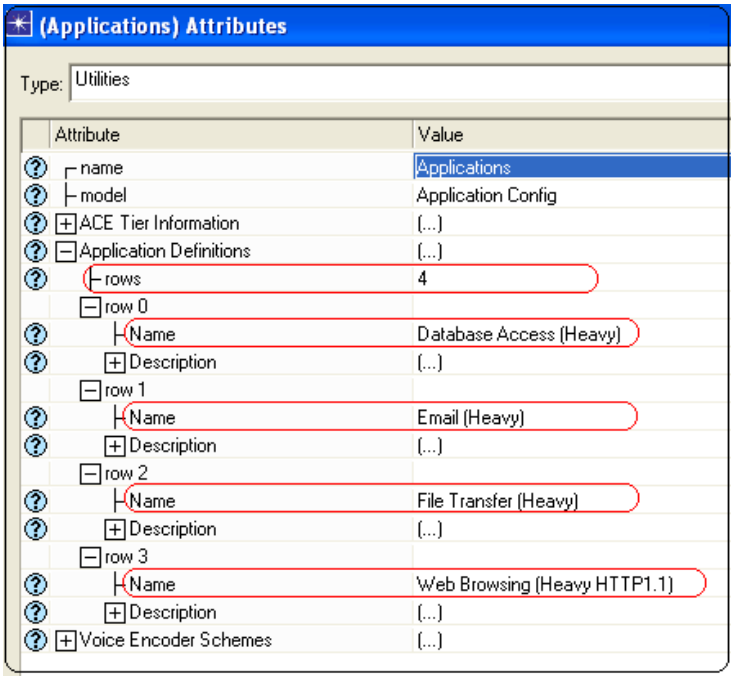
Sistem tasarımında; 5 adet ethernet8_slip_gtwy yönlendirici, 8 adet ethernet16_switch, 7 adet ethernet_server, 7 adet birden fazla iş istasyonunu (workstation) temsil eden 10BaseT_LAN ve dışarıdan erişimi göstermek için 1 adet Ethernet iş istasyonu (workstation) ve bileşenler arası bağlantıyı sağlamak için 10BaseT_LAN ve PPP Internet bağlantı kablosu kullanılmıştır. Bu yapıda 10 Mb veri hızını desteklenmektedir.

Yapıda uygulamalar ve bu uygulamaların hangi kullanıcılar tarafından kullanılacağının tanımını yapmak için '**Application Config**' ve '**Profile Config**' bileşenleri eklenmiştir. Bu aşamadan sonra yapılacak işlem, sistemde gerçekleştirilecek uygulamaların tanımlanması ve hangi bileşenlerin hangi uygulamalar için kullanılacağının belirlenmesidir.

6.3.1. Güvenlik Yapıları Olmayan Senaryonun OPNET Ayarları

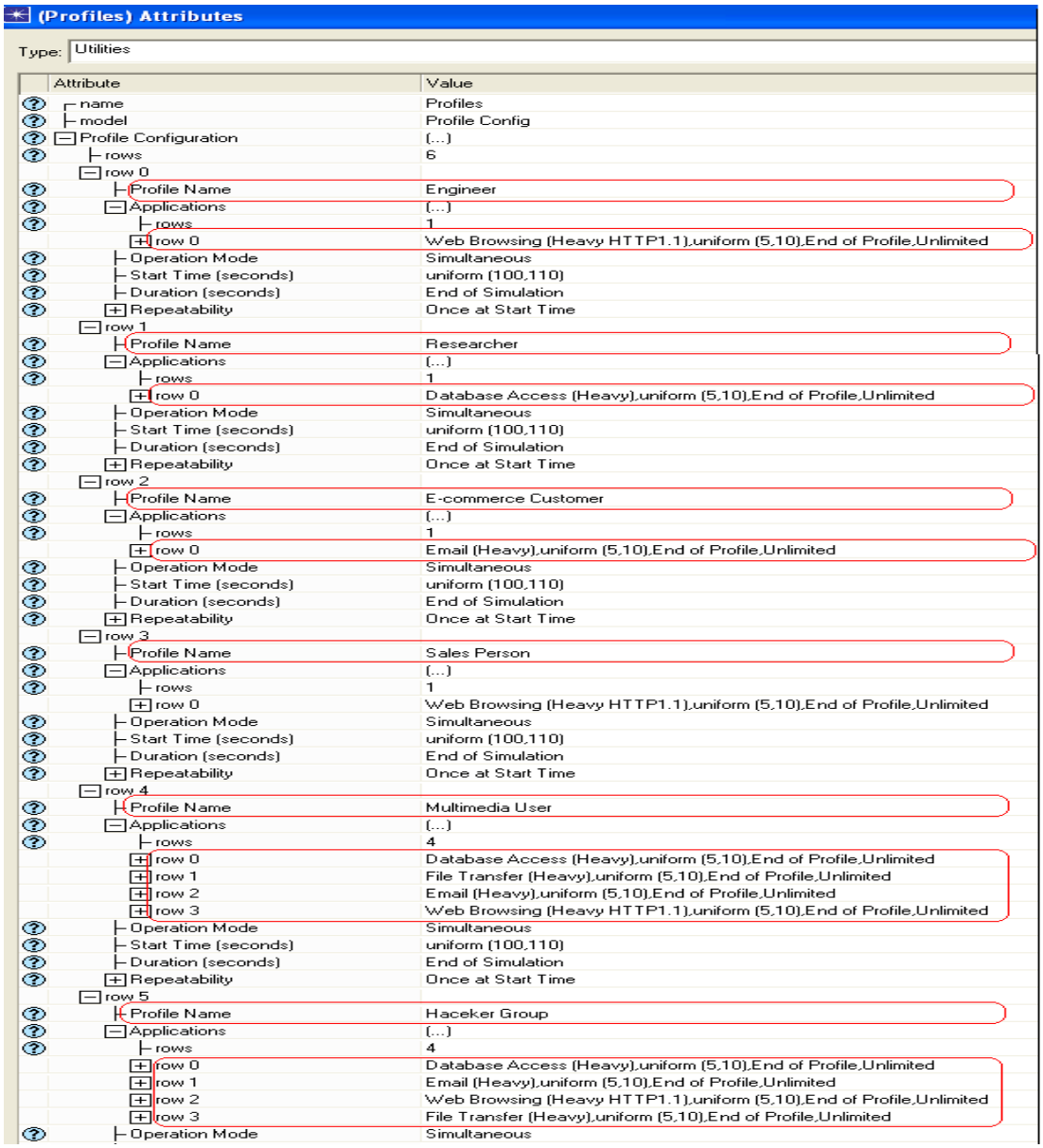
Kurum ağında beş farklı sunucu ve 385 farklı kullanıcı olacaktır. Bunların dışında sisteme dışarıdan dahil olmaya çalışan biri (hacker) mevcuttur. Kullanılan sunucular FTP, HTTP, posta ve veritabanı sunucuları olacaktır. Her bir kullanıcı gurubu bu hizmetlerden bazılarına erişebilirken, hacker ise tüm hizmetlerden faydalanabilecektir. Bu özelliklere göre uygulama ve profil ayarları tanımlanmalıdır.

Ağda kullanılacak uygulamalar '**Application Config**' nesnesi vasıtasıyla tanımlanmaktadır. Bu OPNET projesi FTP, HTTP, posta ve veritabanı olmak üzere dört uygulama ile gerçekleştirilmiştir ve '**Application Config**' üzerinden bu dört uygulamanın her biri için 'Heavy' özelliği seçilmiştir. Şekil 6.2'de '**Application Config**' nesnesinin ayarları görülmektedir.



Şekil 6.2. 'Application Config' nesnesi üzerindeki uygulama ayarları.

‘**Application Config**’ nesnesinde tanımlanan uygulamaların, hangi kullanıcılar tarafından kullanacağının tanımlanması için “**Profiles Config**” nesnesini kullanıyoruz. ‘Profiles Config’, OPNET üzerinde kullanılan “**Ethernet Workstation**” gibi bileşenlerin hangi profil kullanarak hangi uygulamayı destekleyeceklerini tanımlandığı kısımdır. Bu yapı için ‘**Engineer**’, ‘**Researcher**’, ‘**E-Commerce Customer**’, ‘**Sales Person**’, ‘**Multimedia User**’ ve ‘**Hacker Group**’ olmak üzere altı profil oluşturulmuştur. “**Profiles Config**” tanımlamaları Şekil 6.3’te görülmektedir [9].



Şekil 6.3.’Profiles Config’ nesnesi üzerindeki ayarlar.

6.3.2. Kullanıcı Profil Yapıları

Projemizde kullandığımız dış sunucu modelindeki posta sunucusu, veritabanı sunucusu, genel ağ (Internet) sunucusu, dosya aktarım sunucusu ve **10BaseT_LAN**, Ethernet iş istasyonu (workstation) nesnelerinin tanımları yapılarak nesnelerin yapacakları görevleri belirlemek gerekiyor. Bu nesneler kullanıcılar ve sunucular olmak üzere iki kısımdan oluşmaktadır.

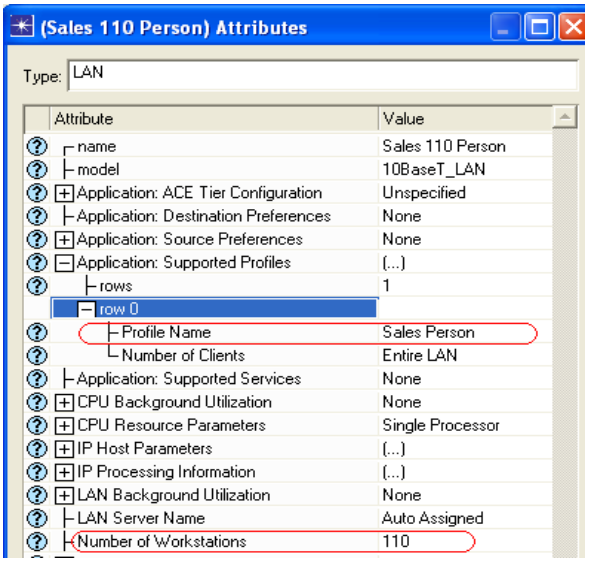
I - Kullanıcı Ayarları:

Simülasyon üzerinde kullanıcı gruplarını ifade eden **10BaseT_LAN** ve Ethernet iş istasyonu (workstation) nesnelerinin tanımlarıdır. Bu nesnelerde, daha önce tanımladığımız "**Profiles Config**" içersindeki '**Engineer**', '**Researcher**', '**E-Commerce Customer**', '**Sales Person**', '**Multimedia User**' ve '**Hacker Group**' uygulamalarından hangilerinin kullanılacağı tanımı yapılır. Kullanıcı profillerinin eriştiği uygulamalar Tablo 6.1'de, nesnelerinin yapılanışı ise Şekil 6.4 ve Şekil 6.5'de verilmiştir.

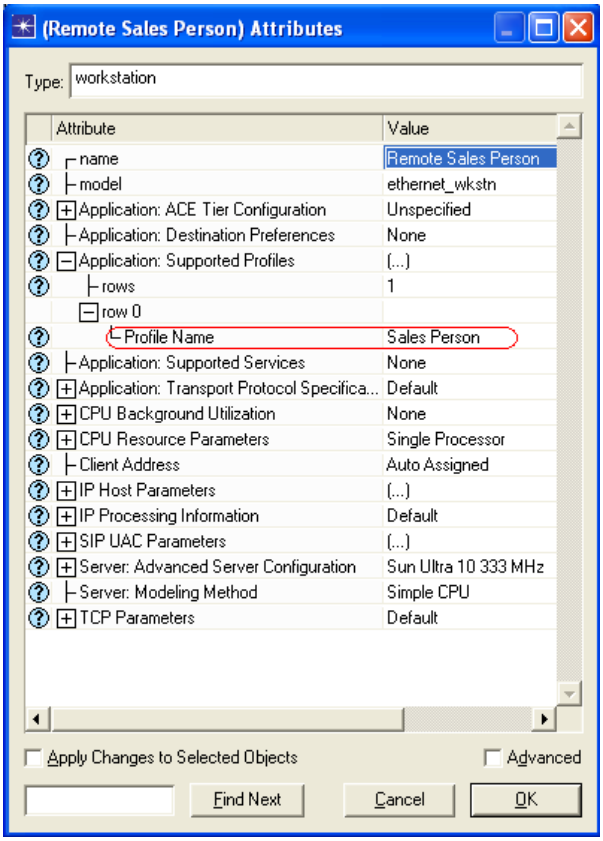
Şekil 6.1. Kullanıcı profillerinin kullandığı uygulamalar.

Profile Adı	**Kullandığı Uygulamalar**
Engineer	'Web Browsing'
Researcher	'Database Access'
E-Commerce customer	'Email'
Sales Person	'Database Access', 'File Transfer'
Multimedia User	'Web Browsing'
Hacker Group	'Web Browsing', 'Database Access', 'Email', 'File Transfer'

10_BaseT_LAN nesnesi birden fazla kullanıcıyı ifade ederken **ethernet_wrkstn** bir kullanıcıyı ifade etmektedir. Her iki nesnede '**rows**' alanı düzenlenerek bir veya birden fazla uygulama kullanılması sağlanabilir. **10_BaseT_LAN** nesnesinin '**number of workstation**' parametresi ile nesnenin kaç kullanıcıya karşılık geleceği değeri ayarlanır.



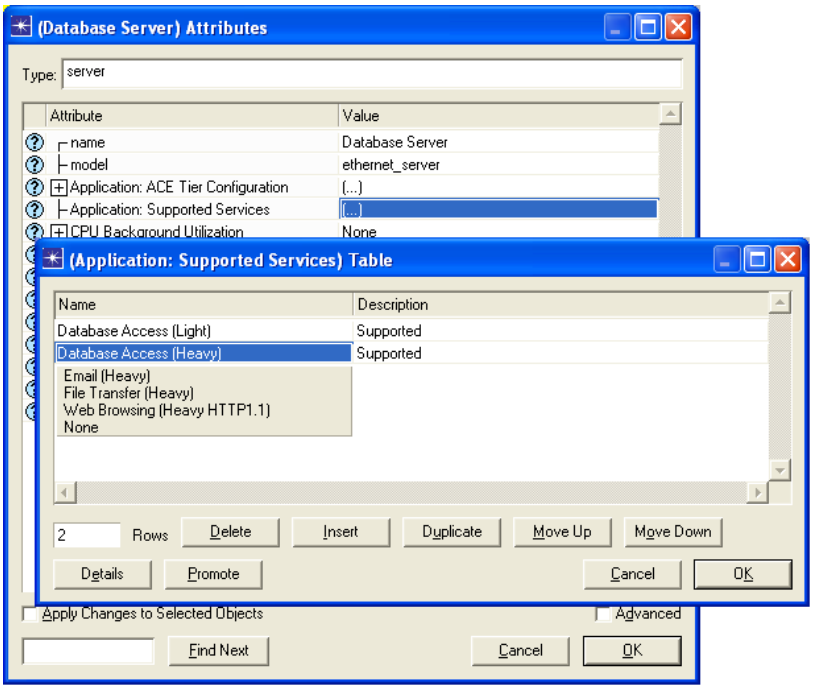
Şekil 6.4. '10BaseT_LAN' nesnesinin yapılanışı.



Şekil 6.5. 'ethernet_wkstn' nesnesinin yapılanışı.

II - Sunucu Ayarları:

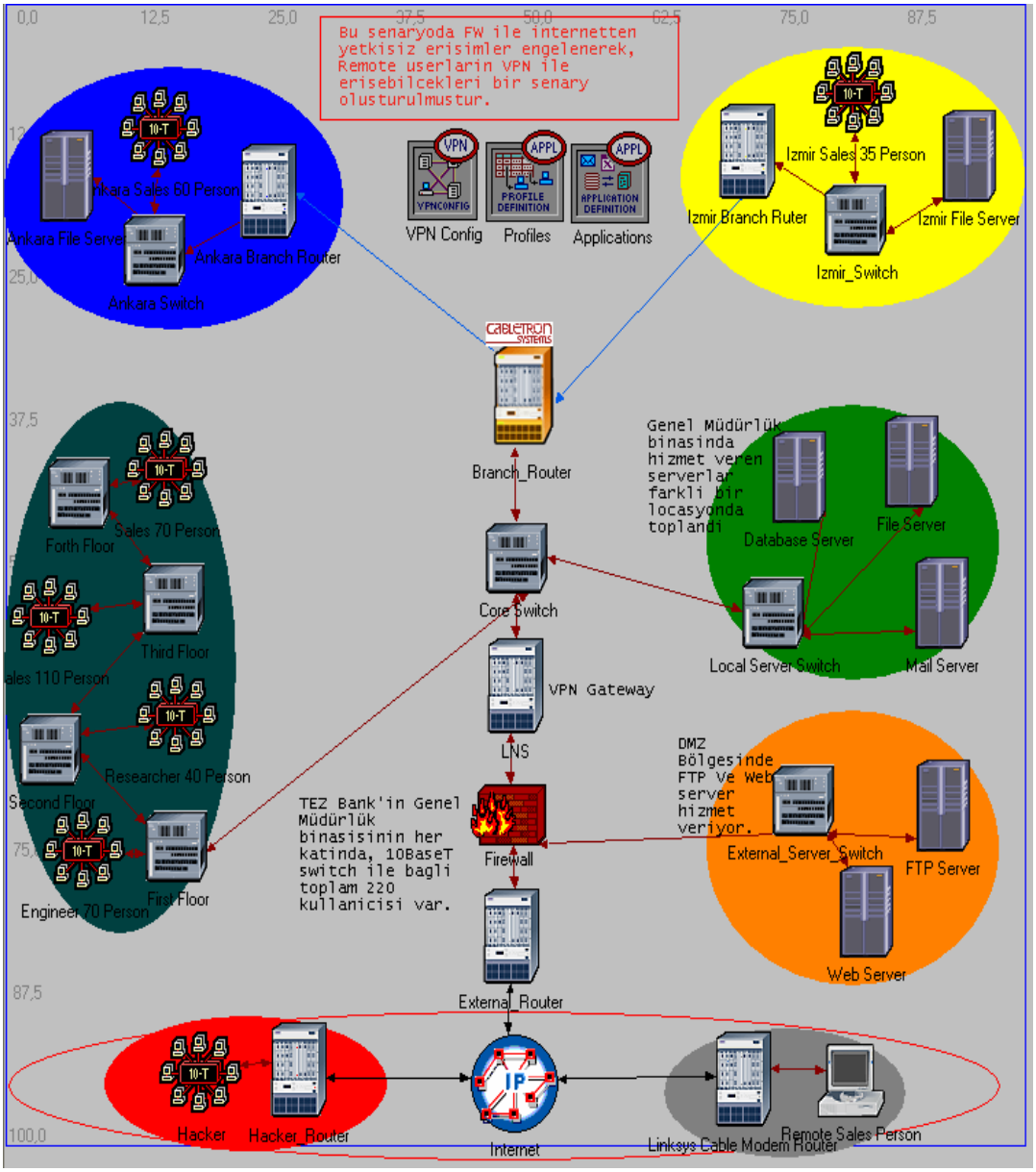
Senaryomuzda beş adet '**ethernet_server**' nesnesi kullanıyoruz. Bu nesnelerden hangisinin, hangi uygulama için servis vereceği ayarının yapılması gerekir. Projemizdeki '**ethernet_server**' nesneleri Şekil 6.6'da olduğu gibi hizmet vereceği sunucu ismi verilerek nesne ismi değiştirilir, '**ethernet_server**' nesnesinin '**Applicator Suported Server**' değerine hizmet vereceği servis veya servisler atanarak düzenlemeleri yapılır. Kullanıcı yapılandırmaları gerçekleştirildikten sonra Firewall_VPN_NO senaryosu tamamlanmış olur.



Şekil 6.6. 'Ethernet_server' nesnesine servis atanması.

6.4. Güvenlik Duvarı ve VPN Kullanarak (Firewall_VPN) Oluşturulan Kurum Ağı

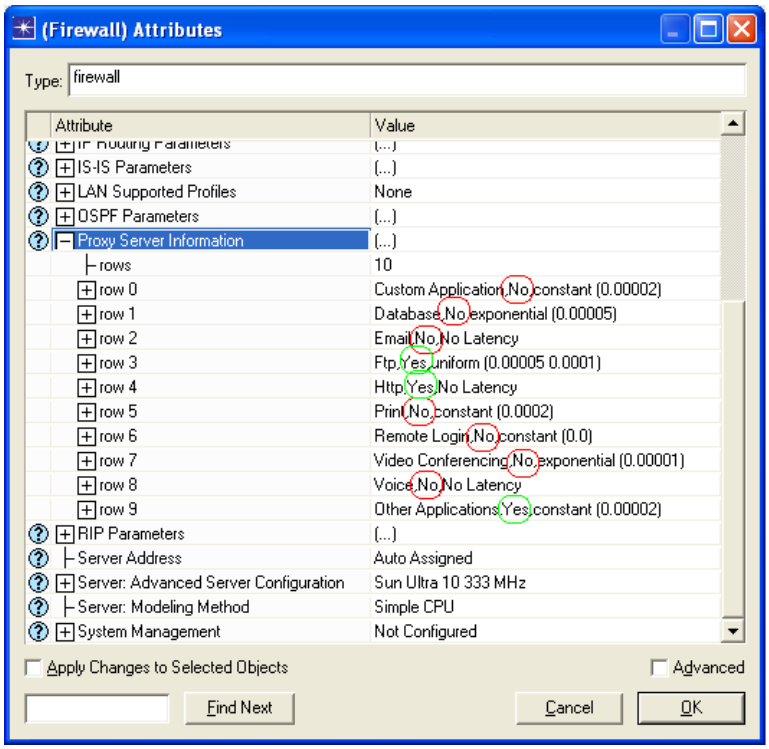
Firewall_VPN_NO senaryomuzu oluşturduktan sonra, aynı senaryonun Güvenlik Duvarı ve VPN içeren şeklini simülasyonunu yapmak için senaryonun bir kopyası alınarak **Firewall_VPN** ismi verilir. Bu senaryodaki amacımız; simülasyonunu yaptığımız kurum yapısına bir tane güvenlik duvarı ve yönlendirici ekleyerek, güvenlik açısından kritik olan LAN ortamının dış dünyadan yalıtılmasını ve şirket dışında bulunan uzak kullanıcıların VPN üzerinden kuruma erişmesini sağlamak. Şekil 6.7'de **Firewall_VPN** senaryosunun ağ diyagramı yer almaktadır.



Şekil 6.7. 'Firewall_VPN' senaryosu network diyagramı.

6.4.1. Güvenlik Duvarı Nesnesinin Yapılanışı

Yapımıza Güvenlik Duvarını ekledikten sonra DMZ bölgesi olarak nitelendirdiğimiz ve dışarıya açık sistemler olan Web ve FTP sunucusunun bulunduğu anahtarı (switch) Güvenlik Duvarı'na bağladık. Güvenlik Duvarı nesnesi üzerinden FTP sunucusu, Web sunucusu ve VPN erişimi dışındaki tüm erişimleri engelledik. Böylelikle kurum dışından kurum iç ağa erişim engellenmiş oldu. Şekil 6.8'de Güvenlik Duvarı nesnesinin özellikleri ve uygulanan kurallar yer almaktadır [29].



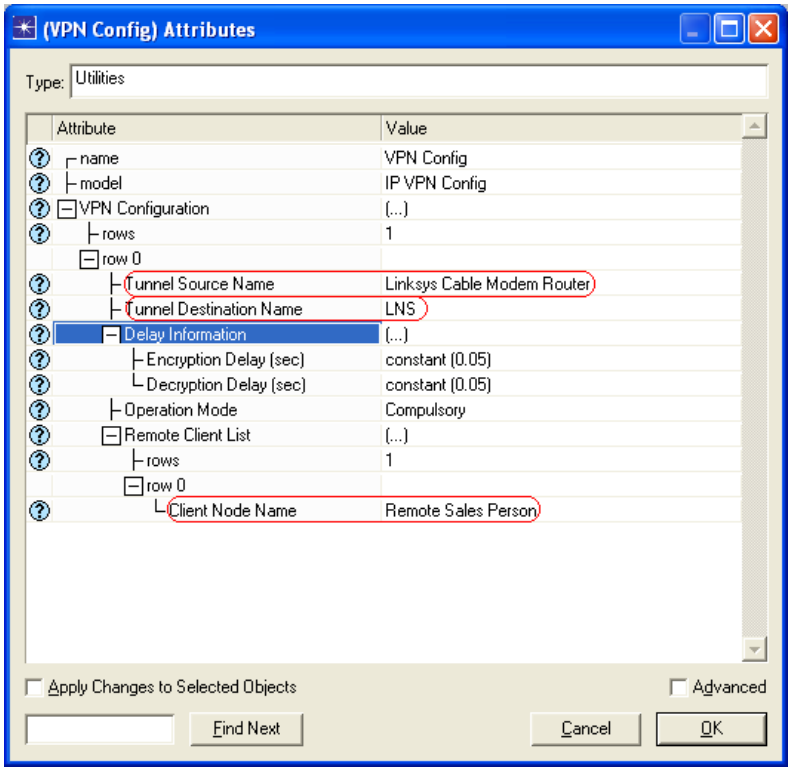
Şekil 6.8. Güvenlik duvarı üzerinde uygulanan kurallar.

Güvenlik Duvarı'nın '**Proxy Server Information**' özelliği altındaki 'rows' tanımları ile uygulamların kuralları belirlenir. Engelenen uygulamalar kırmızı, izin verilenler ise yeşil renkle gösterilmektedir.

6.4.2. 'VPN Config' Nesnesinin Yapılanışı ve VPN Ayarları

Kurum ağının güvenlik duvarını yapıya geçirdikten sonra kurum dışından hiçbir şekilde Kurum Yerel Ağı'na erişim mümkün olmamaktadır. Kurumun uzak çalışanlarının kurum kaynaklarına erişimi için simülasyonumuzda '**Internet Tool Box'** paletinde yer alan '**VPN Config**' nesnesini kullanıyoruz. Bu nesne ile bir veya birden fazla yönlendirici arasında VPN tanımı yapılabiliyor. Şekil 6.9'da '**VPN Config**' nesnesinin yapılanışı yer almaktadır.

Senaryodaki iki cihazın VPN tünel oluşturabilmeleri için '**VPN Config**' nesnesinin 'VPN Configuration' özelliğinin '**rows**' değeri 1 yapılır ve açılan '**row 0**' alanında VPN yapacak yönlendiriciler, kaynak ve hedef alanına tanımlanır. Bu işlem ile yönlendiriciler arasında VPN tanımı yapılmış olur, fakat yönlendiriciye bağlı kullanıcıların kuruma erişebilmeleri için '**Client Node Name**' alanına erişim yapacak kullanıcıların girilmesi gerekmektedir.



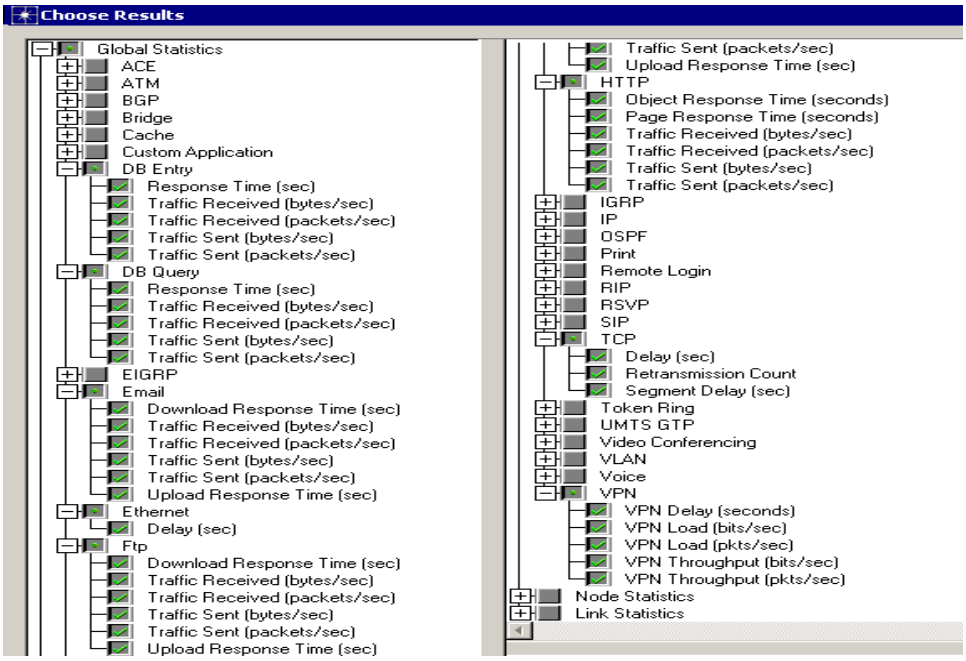
Şekil 6.9. 'VPN Config' nesnesinin ayarları.

6.5. Analizler ve Sonuçlarının Karşılaştırılması

Senaryolarımızı tamamladıktan sonra, oluşturduğumuz senaryolarda simülasyon sonuçlarını karşılaştırabilmemiz için hangi verilerin toplanması gerektiğine karar verilmesi gerekiyor. Temel olarak HTTP, veritabanı, posta, dosta aktarım ve IP verilerini hesaplayacağız. Şekil 6.10'da toplanmasını istediğimiz **Global Statics** verileri yer almaktadır. Simülasyonun çalışması bittikten sonra aşağıdaki rapor bilgisi oluşmuştur:

Firewall_VPN senaryosunun rapor çıktısı;

```
Beginning simulation at 02:37:16 Paz Haz 06 2010
Simulation Completed - Collating Results.
Events: Total (18389868), Average Speed (279893 events/sec.)
Time: Elapsed (1 min. 5 sec.), Simulated (5 min. 0 sec.)
Simulation Log: 497 entries
```



Şekil 6.10. Simülasyon sırasında toplanacak değerler.

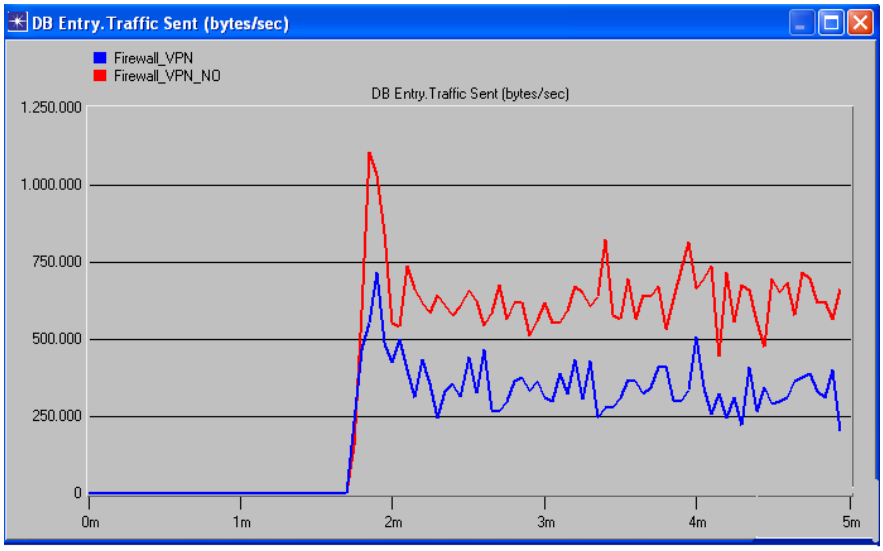
Firewall_VPN_NO senaryosunun rapor çıktısı;

```
Beginning simulation at 02:38:28 Paz Haz 06 2010
Simulation Completed - Collating Results.
Events: Total (23348353), Average Speed (249592 events/sec.)
Time: Elapsed (1 min. 33 sec.), Simulated (5 min. 0 sec.)
Simulation Log: 10 entries
```

Bu bilgilere, göre **Firewall_VPN_NO** senaryosunun çalışma süresi 1 dakika 33 saniyedir. Gerçekleşen toplam olay sayısı 23.348.353'tür. **Firewall_VPN** senaryosunun çalışma süresi ise 1 dakika 5 saniyedir. Gerçekleşen toplam olay sayısı 18.389.868'dir. Bu iki çıktıyı karşılaştırdığımız zaman Güvenlik Duvarı ve VPN kullanımıyla iç ağa yansıyan olay sayısının yaklaşık olarak % 21.2 oranında azaldığını gözlemlemekteyiz.

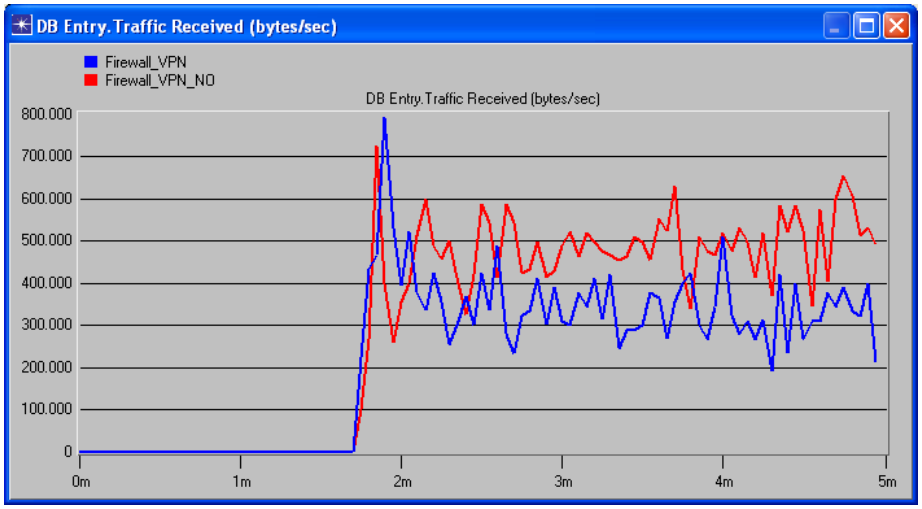
6.5.1. DB Entry Simülasyon Grafikleri

Güvenlik Duvarı olmadan önce sistem herkese açık olduğu için bu senaryoda DB Entry'nin '**Trafic Sent**' değeri Şekil 6.11'deki grafikten de görülebileceği gibi ortalama %25 oranında daha düşüktür. **Firewall_VPN_NO** simülasyonunda saniyede ortalama 600.000 byte gözlenirken, **Firewall_VPN** simülasyonunda bu değer 450.000 byte civarındadır.

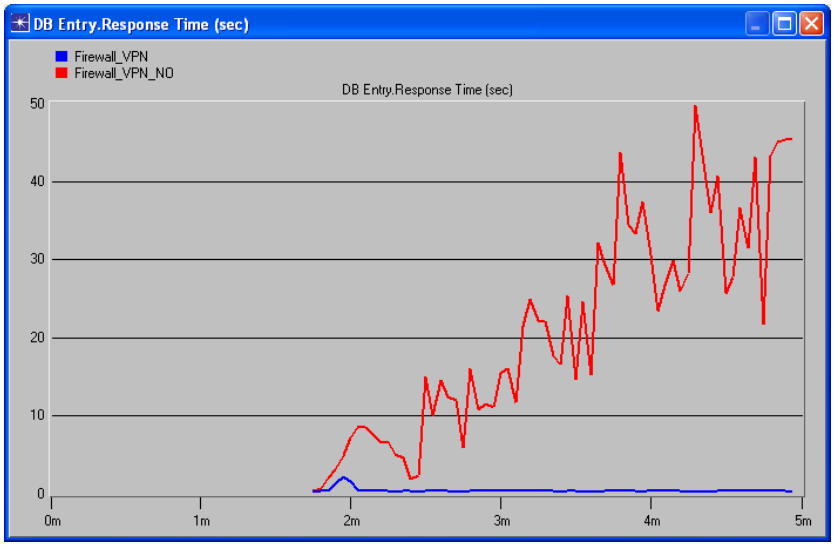


Şekil 6.11. DB Entry'nin 'Trafic Sent' grafiği.

Yapılan analizler sonucunda Şekil 6.12 ve Şekil 6.13'te kurum dışından gelen trafiğin güvenlik duvarı tarafından kesilmeden ve kesilerek yapılan simülasyonun DB Entry üzerindeki etkileri görülmektedir. Kırmızı ile mavi grafikler arasında çok büyük farklar vardır. Bu da güvenlik duvarının beklenen etkiyi gösterdiğini, kurum dışından '**Hacker Group**' olarak tanımladığımız kaynaklara izinsiz erişmek isteyen kişileri kestiğini göstermektedir. Güvenlik duvarının olmadığı simülasyon ortamı ile güvenlik duvarının olduğu simülasyon ortamları arasında iki kattan daha fazla trafik olduğu buradaki sonuçtan dolayı kurum ağlarının güvenlik duvarı gibi güvenlik sistemleri ile korunması gerektiğini söyleyebiliriz.



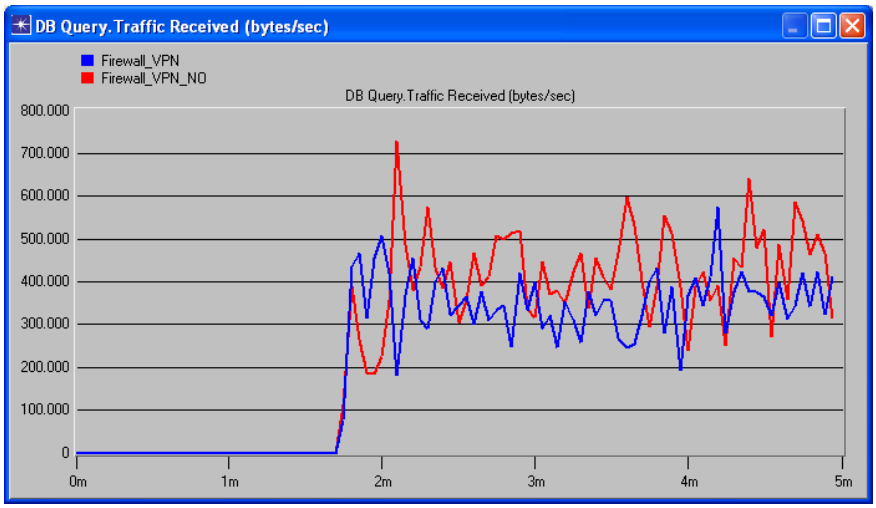
Şekil 6.12. 'DB Entry Trrafic Received' grafiği.



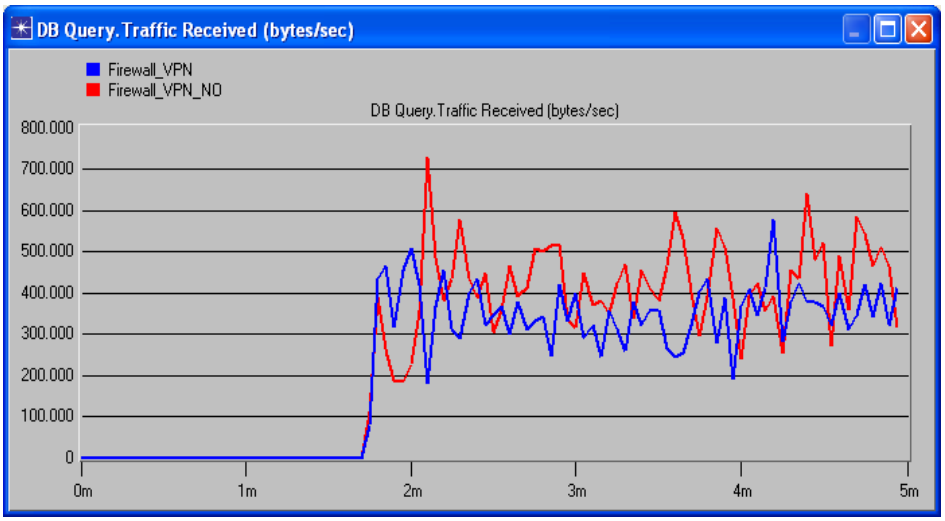
Şekil 6.13. 'DB Entry Response Time' grafiği.

6.5.2. DB Query Simülasyon Grafikleri

DB Entry'de olduğu gibi DB Query üzerinde de Güvenlik Duvarının etkisi açık olarak görülmektedir. Şekil 6.14'te '**Trafic Sent**' ve Şekil 6.15'te '**Trafic Receive**' grafikleri görülmektedir. Bazı noktalarda **Firewall_VPN_NO** senaryosunun değerlerinin **Firewall_VPN** senaryosundaki değerlerden daha düşük olduğu gözlenmektedir. Bu da kurum içi ağ kullanımının anlık olarak kurum dışından gelen isteklerden daha yoğun olduğu test anı olarak düşünülebilir. Her üç grafiğe bakıldığında, Güvenlik Duvarı ve VPN ile yetkisiz erişimlerin engellenerek kurum ağ performansının ve kurum güvenliğinin daha üst seviyeye taşındığını görebiliriz.



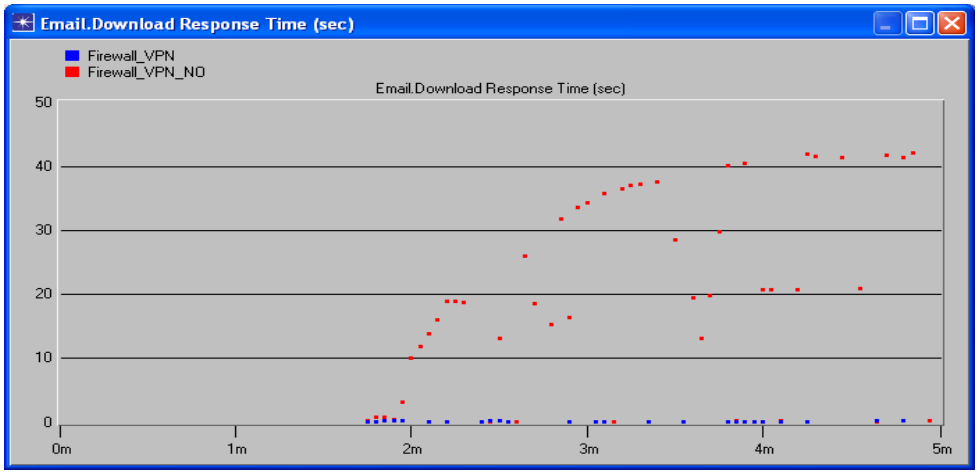
Şekil 6.14. 'DB Query Trafic Sent' grafiği.



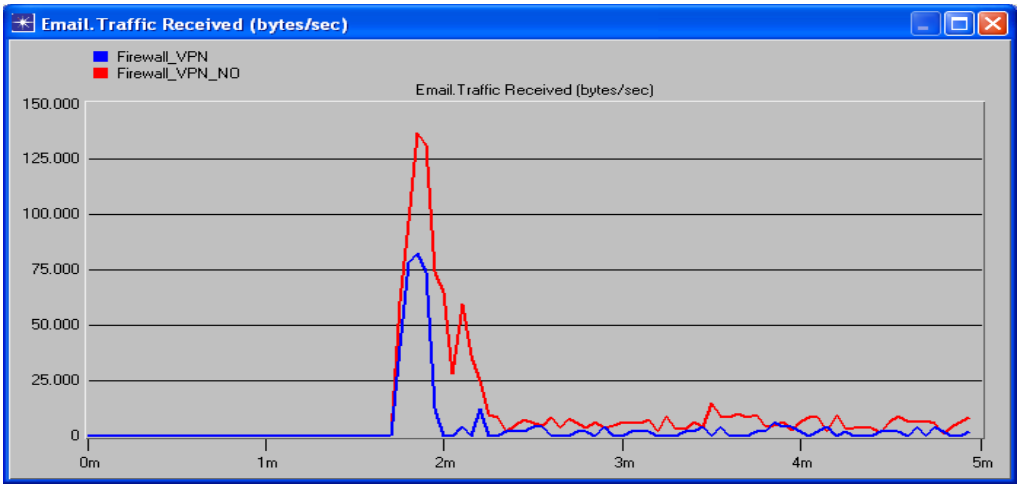
Şekil 6.15. 'DB Quey Trafic Received' grafiği.

6.5.3. E-Posta Simülasyon Grafikleri

Güvenlik Duvarı olmadığı zaman DB Entry ve DB Query değerlerinde olduğu gibi e-posta analizleri de güvenlik duvarının olmasından olumlu etkilenmiştir. '**Download Response Time**' değerlerinin güvenlik duvarı olmayan simülasyonda, Şekil 6.16'dan görülebileceği gibi, 40 saniyenin üzerine çıktığı gözlenmektedir. Şekil 6.17'de ise saniyedeki posta trafiği 125.000 byte'in üzerine çıkmaktadır. Güvenlik duvarı ve VPN kullanımı ile kurum ağı üzerindeki e-posta sunucusunun yetkisiz erişimlere kapatıldığı görülmektedir.



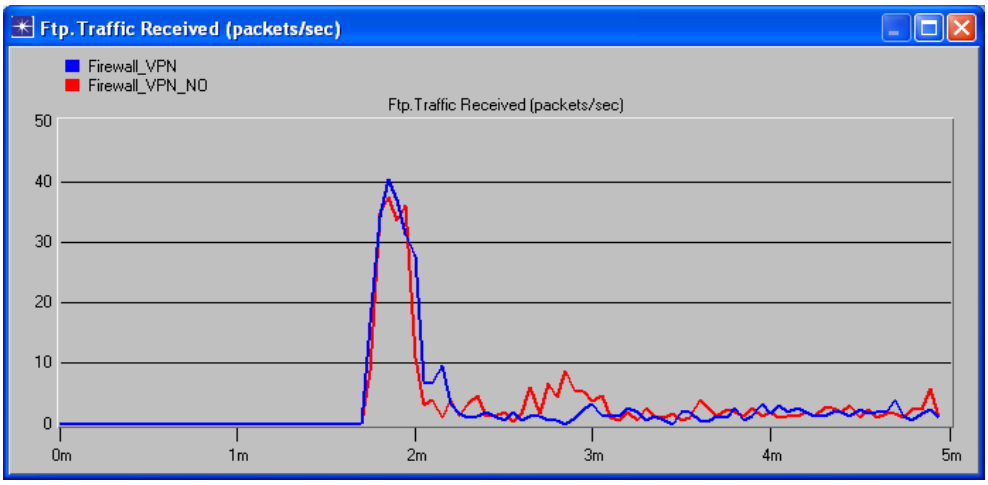
Şekil 6.16. 'Email Download Response Time' grafiği.



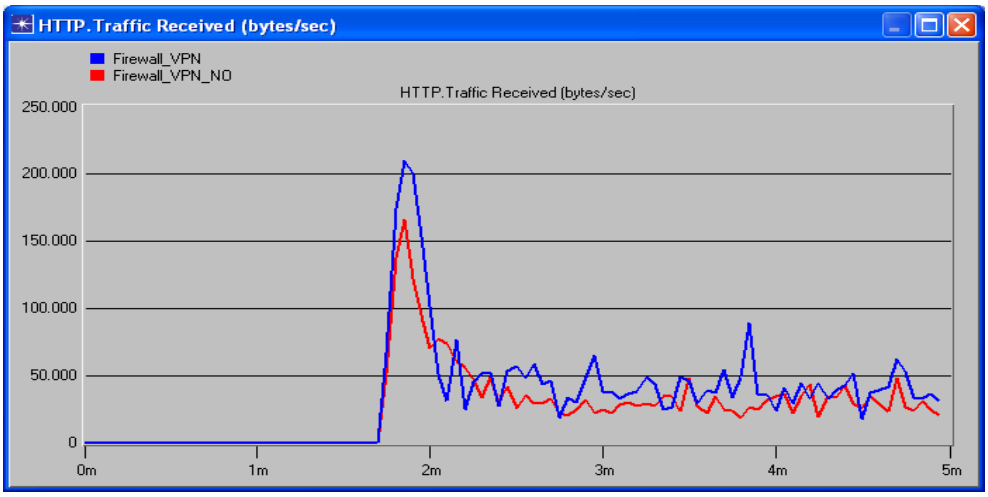
Şekil 6.17. 'Email Trafic Received' grafiği.

6.5.4. HTTP Sunucusu ve FTP Sunucusu Simülasyon Grafikleri

Güvenlik Duvarı üzerinde HTTP ve FTP sunucularına erişim için bir engelleme koyulmadığı için iki sümülasyon sonuçları arasında fark beklenmemekteydi. Şekil 6.18'daki '**FTP Server Traffic Received**' grafiği ile Şekil 6.19'deki '**HTTP Traffic Received**' sonuçlarının birbirlerine yakın olduğu gözlenmiştir. Bu grafikler dikkate alındığında, Güvenlik Duvarı kullanılamayacak durumlar için Saldırı Tespit Sistemleri gibi daha farklı güvenlik yapıları kullanarak, kurum ağ sistemleri saldırılara karşı korunması gerektiği anlaşılmaktadır.



Şekil 6.18. 'FTP Server Traffic Received' grafiği.



Şekil 6.19. 'HTTP Traffic Received' grafiği.

7. SONUÇ

Bu tezde önce bir temel kurumsal ağın gerçek ortamı oluşturuldu ve üzerinde ağ paket ölçümleri ve analizleri yapıldı. Bir VPN bağlantısı üzerinden kurum kaynaklarına erişim gerçekleştirilmiştir. Oluşturulan kurum ağı içerisinde bulunan web sunucusuna, kurum ağı dışında, Internet ortamında bulunan bir bilgisayardan Apache JMeter uygulaması ile istekler gönderiliştir. Gönderilen isteklerin web sunucusu ve ağ üzerindeki etkisi, Wireshark ile toplanan ağ paketleri CACE Pilot uygulaması ile analiz edilmiştir. Analizler sonucunda Web sunucusunun isteklere yanıt süreleri ve ağ trafik değerleri bize karşılaştırma yapabilmemiz açısından bir ölçüm aracı olmuştur.

İkinci olarak gerçek ağ modelinin bir benzerini OPNET simülasyon ortamında gerçekleştirdik ve üzerinde simülasyonlar yaptık. 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 benzerlik gösterdiği ve OPNET simülasyon aracı ile yapılacak çalışma sonuçlarının gerçeğe oldukça yakın sonuçlar ürettiği gözlenmiştir.

Tezimizde üçüncü olarak sadece OPNET ortamında daha gerçekçi bir kurumsal bir ağ modeli geliştirilmiştir. Günümüz önemli güvenlik alt yapıları dikkate alınarak, finansal alanda hizmet veren 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 etikleri incelenmiştir. Günümüz kurumsal ağ yapılarına örnek olabilecek şekilde tasarladığımız kurumsal ağ modelini, Güvenlik Duvarı ve VPN kullanarak ve bunları kullanmayarak simülasyonunun yapılması şeklinde iki farklı senaryo oluşturuldu. İki senaryonun OPNET simülasyon test sonuçları incelenerek, Güvenlik Duvarı ve VPN'in kurum güvenliği ve ağ performansına olan etkileri gösterildi.

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 tasarlanması, simülasyonlarının yapılması ve tasarımlarının doğrulanması, maliyet ve zaman tasarrufu sağlayacaktır.

8. KAYNAKLAR

1. J. Mohorko, F. Matjaž, K. Saša "Advanced Modelling and Simulation Methods for Communication Networks", *Microwave Review*, September, 2008.
2. J. Potemans, B. Van den Broeck, Y. Guan, J. Theunis, E. Van Lil and A. Van de Capelle, "Implementation of an Advanced Traffic Model in OPNET Modeler", *OPNETWORK 2003*, Washington D.C., USA, 2003.
3. J. Felten, O. Gurbuz, H. Owen, T. GroBmann, G. Kussmann, W. Schrock, "Modeling, Simulation and Verification of an Enterprise Network", *Globol Telecommunications Conference – Globecom'99*, 1999.
4. X. Chang, "Network Simulations with OPNET", *Proceedings of the 1999 Winter Simulation Conference*, 1999.
5. A. Zaballos, G. Corral, I. Serra, J. Abella, "Testing Network Security using OPNET", *OPNETWORK'2003*, Washington DC (United States) August 2003.
6. G. Corral, A. Zaballos, J. Abella, C. Morales, "Building an IDS using OPNET", *OPNETWORK'2005*, Washington DC, USA, August 2005.
7. A. Kumar, "Development of Laboratory Exercıses Based on the Opnet Network Simulating Approach", *Rivier College Online Academic Journal*, Vol. 1, No. 1, 2005.
8. J. Theunis, B. Van den Broeck, P. Leys, J. Potemans1, E. Van Lil, A. Van de Capelle, "OPNET in Advanced Networking Education", *OPNETWORK 2002*, Washington D.C., USA, 2002.
9. V. Hnatyshin, A. F. Lobo, P. Bashkirtsev, R. DeDomenico, A. Fabian, G. Gramatges, J. Metting, M. Simmons, M. Stiefel, "Modeling a University Computer Laboratory using OPNET Software", Computer Science Department, Rowan University, New Jersey, United States, 2006.
10. J. Potemans, J. Theunis, M. Teughels, E. Van Lil, A. Van de Capelle, "Student Network Design Projects using OPNET", *OPNETWORK 2001*, Washington D.C., USA, 2001.
11. S. Iyer, N. McKeown, "Analysis of the Parallel Packet Switch Architecture", *IEEE/ACM Transactıons on Networking*, Vol. 11, No. 2, April 2003, pp. 314–324.
12. Netcraft web sitesi: http://news.netcraft.com/ .
13. Microsoft DHCP server, Microsoft web sitesi: http://support.microsoft.com/kb/169289 .
14. QIP DHCP Server, QIP web site: http://qip.com/ .
15. A. K. Jones, S. R. Sielken, "Computer System Intrusion Detection: A Survey", Department of Computer Science, University of Virginia, Charlottesville, VA, USA, 1999.
16. NS-2 web sitesi: http://nsnam.isi.edu/nsnam/index.php/Main_Page .
17. R. Sokullu, M. A. Akkaş, "Ns-2 Eğitimi ve Laboratuar Programı", EEBB Mühendislikleri Eğitimi 4. Ulusal Sempozyumu, 22-24 Ekim 2009.
18. OPNET ana sayfası: http://www.opnet.com/ .
19. Wireshark web sitesi: www.wireshark.org .

20. Softperfect web sitesi: www.softperfect.com .
21. Network Security Scanner web sitesi: www.nmap.org .
22. Grinder web sitesi: grinder.sourceforge.net .
23. Apache Jmeter web sitesi: http://jakarta.apache.org/jmeter/ .
24. CACE Pilot web sitesi: www.cacetech.com .
25. Open suse sitesi: www.opensuse.org .
26. Netfilter web sitesi: www.netfilter.org .
27. Openvpn web sitesi: http://openvpn.net/ .
28. Microsoft DNS Server web sitesi: http://support.microsoft.com/kb/814591 .
29. C. Çakır, H. Kaptan, "VoIP Teknolojilerinde OPNET Tabanlı Güvenlik Uygulaması", *Bilişim Teknolojileri Dergisi*, Cilt 2, Sayı 3, Eylül 2009.