T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

GÜVENLİK DUVARI VE SANAL ÖZEL AĞ ÇÖZÜMLERİNİN AĞ PERFORMANSINA ETKİLERİNİN İNCELENMESİ

SERKAN ÇAM

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI

Tez Danışmanı: Prof. Dr. Gürkan TUNA

EDİRNE-2020

Serkan ÇAM'ın hazırladığı "Güvenlik Duvarı ve Sanal Özel Ağ Çözümlerinin Ağ Performansına Etkilerinin İncelenmesi" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir Yüksek lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri (Ünvan, Ad, Soyad): İmza

Prof. Dr. Gürkan TUNA .....

Dr. Öğr. Üyesi Tarık YERLİKAYA .....

Dr. Öğr. Üyesi Fatih AYDIN .....

Tez Savunma Tarihi: 13/01/2020

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Prof. Dr. Gürkan TUNA
Tez Danışmanı .....

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

.....

Prof. Dr. Murat YURTCAN
Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

13 / 01 / 2020

Serkan ÇAM

İmza

Yüksek Lisans Tezi

Güvenlik Duvarı ve Sanal Özel Ağ Çözümlerinin Ağ Performansına Etkilerinin İncelenmesi

T.Ü. Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

Günümüzde çoğu kuruluş, mevcut sunucu, yazılım ve ağ kaynaklarını internet üzerinden hizmet sunumu için kullanmaktadır. Sunulan bu hizmetler ile ağ üzerinden iletilen bilginin, gizliliği ve güvenliği sağlanmak istenmektedir. Güvenlik, sunulan hizmetlerin önemli bir şartı haline gelmektedir. Bu güvenlik isteği genelde, kaynaklara erişimin yetkilere göre kısıtlanmasını, olası internet ve ağ üzerinden gelebilecek sanal saldırılara karşı koruma sağlanmasını kapsamaktadır. Bu istekleri yerine getirmek için güvenlik duvarı ve sanal özel ağ çözümleri kullanılmaktadır.

Güvenlik duvarı, merkezi bir noktada bulunarak gelen ve giden ağ trafiğine istenen güvenlik kurallarının uygulanmasını sağlamaktadır. Bu yönden bir güvenlik duvarı, kurala uyan trafiğe izin veren, uymayanları ise engelleyen bir rol üstlenmektedir. Sanal özel ağlar, internet gibi genel ve paylaşımlı bir ağ üzerinden kontrollü bir bağlantı sağlamaktadır. Bu işlemi yaparken iki uç düğüm arasındaki bilgi iletişimini IP tüneli adı verilen sanal bağlantılar kullanarak gerçekleştirir. Bilindiği üzere, güvenlik duvarı ve sanal özel ağların kullanımı ağda performans ile ilgili çeşitli değişikliklere yol açmaktadır. Bu performans değişikliklerinin gözlemlenmesi, ağ sisteminin güncelliğinin ve ihtiyaçlarının analizi açısından çok önemlidir.

Bu tez çalışmasında güvenlik duvarı ve sanal özel ağ çözümlerinin ağ performansına olası etkileri OPNET benzetim programında oluşturulan senaryolar yardımı ile açıklanmaktadır.

Yıl : 2020

Sayfa Sayısı : 118

Anahtar Kelimeler : Güvenlik Duvarı, Sanal Özel Ağ, Ağ Performansı, OPNET

Master Thesis

Examining of the Effects of Firewalls and Virtual Private Network Solutions on Network Performance

Trakya University Institute of Natural Sciences

Computer Engineering

ABSTRACT

Nowadays, most organizations use existing servers, software and network resources to provide services over the Internet. With these services, confidentiality and security of the information transmitted over the network is desired. This security request generally includes restricting access to resources according to authorizations and providing protection against possible internet and network attacks. Firewall and virtual private network solutions are used to fulfill these requests.

The firewall is located at a central point, allowing the required security rules to be applied to incoming and outgoing network traffic. In this respect, a firewall plays a role that allows traffic that obeys the rule and prevents those who do not. Virtual private networks provide a controlled connection over a public and shared network, such as the Internet. During this connection, they perform communication between two end nodes using virtual connections called the IP tunnel. The use of firewalls and virtual private networks induces various performance changes on the network. Monitoring those changes is crucial in terms of supplying the updates and requirements of the network systems.

This study finds out the possible effects of the firewall and virtual private network solutions on network performance by exploiting the scenarios prepared in the OPNET simulation program.

Year : 2020

Number of Pages : 118

Keywords : Firewall, Virtual Private Network, Network Performance, OPNET

TEŞEKKÜR

Çalışmalarımı yönlendiren ve araştırmalarımın her aşamasında bilgi, öneri ve deneyimleri ile yol gösterip yardımlarını esirgemeyen danışmanım Sayın Prof. Dr. Gürkan TUNA' ya teşekkürlerimi sunarım.

Çalışmalarım esnasında gösterdiği büyük sabırdan dolayı eşim Neşe ÇAM, Kızlarım Eylül Nisa ÇAM ve İlke ÇAM' a içtenlikle teşekkür ederim.

Serkan ÇAM

Edirne,2020

İÇİNDEKİLER

ÖZET iv
ABSTRACT vi
TEŞEKKÜR viii
İÇİNDEKİLER ix
KISALTMALAR xii
ŞEKİLLER xvi
ÇİZELGELER xviii
BÖLÜM 1 1
GİRİŞ 1
1.1. Bilgisayar Ağları ve Ağ Güvenliği 1
1.2. Amaç 3
1.3. Tez Organizasyonu 4
BÖLÜM 2 6
LİTERATÜR ÖZETİ 6
2.1. Bilgisayar Ağlarının Benzetim ile Performans İnceleme Çalışmaları 6
2.2. Bilgisayar Ağlarındaki Güvenlik Çözümlerinin Benzetim Yolu ile Ağ Performansına Olan etkilerini İnceleyen Çalışmalar 7
BÖLÜM 3 10
GENEL BİLGİLER 10
3.1. Referans Modeller 10
3.1.2. OSI Referans Modeli 11

3.1.3. TCP/IP Referans Modeli 13
3.2. Ağ Yapıları 18
3.2.1. Mantıksal Ağ Topolojileri 18
3.2.2. Fiziksel Ağ Modelleri 19
3.2.3. Coğrafi Kapsamlarına Göre Ağ Türleri 21
3.2.4. Kurumsal Ağlar 22
3.3. Ağ Güvenliği 24
3.4. Güvenlik Duvarları 24
3.4.1. Paket Filtrelemeli Güvenlik Duvarı 25
3.4.2. Uygulama Katmanı Güvenlik Duvarı 26
3.4.3. Durum Denetimli Güvenlik Duvarı 27
3.5. Sanal Özel Ağlar 28
3.5.1. Uzaktan Erişim Sanal Özel Ağ 29
3.5.2. Siteden Siteye Sanal Özel Ağlar 29
3.5.3. Sanal Özel Ağ Tünelleme Protokolleri 30
3.5.3.1. IPSec 31
3.5.3.2 PPTP 31
3.5.3.3. L2TP 31
3.5.3.4. SSL/TSL 32
BÖLÜM 4 33
AĞ MODELLEME/BENZETİM VE OPNET 33
4.1. Benzetim ve Modelleme Araçları 34
4.2. OPNET Modeler 36
4.2.1. OPNET Modeler Düzenleyicileri 37
4.2.1.1. Proje Düzenleyici 37
4.2.1.2. Düğüm Düzenleyici 38

4.2.1.3. Süreç Düzenleyici 39
BÖLÜM 5 42
METODOLOJİ 42
5.1. OPNET ile Ağın Modellenmesi 42
5.2. Ağ Modelinin Ayarlarının Yapılması 44
5.2.1. Güvenlik Duvarı ve Sanal Özel Ağ Etkin Olmayan Senaryonun Ayarları 45
5.2.2. Toplanacak İstatistik Verilerinin Seçilmesi 49
5.2.3. Güvenlik Duvarı Etkin, Sanal Özel Ağ Etkin Olmayan Senaryonun Ayarları 50
5.2.4. Güvenlik Duvarı ve Sanal Özel Ağ Etkin Olan Senaryonun Ayarları 51
5.2.5. Benzetim İşleminin Başlatılması 53
5.3. Elde Edilen İstatik ve Grafikler 54
BÖLÜM 6 62
SONUÇLAR ve TARTIŞMA 62
6.1. Katkıları 63
6.2. Öneriler 63
KAYNAKLAR 65
EKLER 72
ÖZGEÇMİŞ 100

KISALTMALAR

ARP	Adres Çözümleme Protokolü (Address Resolution Protocol)
ARPA	Gelişmiş Araştırma Projeleri Ajansı (Advanced Research Projects Agency)
ATM	Eş zamansız Aktarım Modu(Asynchronous Transfer Mode)
CRC	Döngüsel Artıklık Denetimi (Cyclic Redundancy Check)
DoD	Amerika Birleşik Devletleri Savunma Bakanlığı (U.S. Department of Defense)
FTP	Dosya Aktarım Protokolü (File Transer Protocol)
HTTP	Hiper Metin Aktarım Protokolü (Hyper-Text Transfer Protocol)
IANA	İnternet Atanan Numaralar Kurumu (Internet Assigned Numbers Authority)
ICMP	İnternet Kontrol Mesaj Protokolü (Internet Control Message Protocol)
IDS	Saldırı Tespit Sistemi (Intrusion Detection Systems)

IEEE	Elektrik-Elektronik Mühendisleri Enstitüsü (The Institute of Electrical and Electronics Engineers)
IP	İnternet Protokolü (Internet Protocol)
IPSec	İnternet Protokolü Güvenliği (Internet Protocol Security)
IPv4	İnternet Protokol Sürüm 4 (Internet Protocol Version 4)
IPv6	İnternet Protokol Sürüm 6 (Internet Protocol Version 6)
IPX/SPX	Ağlar Arası Paket Değişimi / Sıralı Paket Değişimi (Internetwork Packet Exchange/Sequenced Packet Exchange)
ISO	Uluslararası Standartlar Teşkilatı (International Organization for Standardization)
İSS	İnternet servis sağlayıcısı
L2TP	İkinci Katman Tünelleme Protokolü (Layer 2 Tunneling Protocol)
LAN	Yerel Alan Ağı (Local Area Network)
MAC	Ortam Erişim Kontrolü (Media Access Control)
MPLS	Çoklu Protokol Etiket Anahtarlama (Multi Protocol Label Switching)

OPNET	Optimize Ağ Mühendislik Aracı (Optimized Network Engineering Tool)
OSI	Açık Sistem Ara Bağlantısı (Open Systems Interconnection)
OSPF	İlk Açık Yöne Öncelik (Open Shortest Path First)
OSPFv3	İlk Açık Yöne Öncelik Sürüm 3 (Open Shortest Path First Version 3)
PPP	Noktadan Noktaya Protokolü (Point-to-Point Protocol)
PPTP	Noktadan Noktaya Tünelleme Protokolü (Point-to-Point Tunneling Protocol)
QoS	Hizmet Kalitesi (Quality of Service)
RFC	Açıklama İstekleri (Request for Comments)
RIR	Bölgesel İnternet Kayıtçısı (Regional Internet Registry)
SSL	Güvenlik Giriş Katmanı (Secure Sockets Layer)
STP	Yayılan Ağaç Protokolü (Spanning Tree Protocol)
TCP	Aktarım Denetim Protokolü (Transmission Control Protocol)
TLS	Taşıma Katmanı Güvenliği (Transport Layer Security)
UDP	Kullanıcı Veri Bloğu Protokolü (User Datagram Protocol)

URL	Tekdüzen Kaynak Konumlayıcı (Uniform Resource Locator)
VLAN	Sanal Yerel Alan Ağı (Virtual Local Area Network)
VoIP	İnternet Protokolü Üzerinden Ses (Voice Over Internet Protocol)
VPN	Sanal Özel Ağ (Virtual Private Network)
WAN	Geniş Alan Ağı (Wide Area Network)
WiMAX	Yeni Çok Hızlı Kablosuz Ağ (Worldwide Interoperability for Microwave Access)
WLAN	Kablosuz Yerel Alan Ağı (Wireless Local Area Network)

ŞEKİLLER

Şekil 1.1. Zararlı yazılımların 1984-2018 arası artışı 3
Şekil 3.1. Yedi katmanlı OSI mimarisi 12
Şekil 3.2. TCP/IP ve OSI katmanları karşılaştırması. 14
Şekil 3.3. Örnek IPv4 paketi (Postel, 1981b). 16
Şekil 3.4. IPv6 başlık biçimi 17
Şekil 3.5. Fiziksel ağ topoloji örnekleri 20
Şekil 3.6. Örnek yerel alan ağı 22
Şekil 3.7. Kurumsal ağ yapısı örneği 23
Şekil 3.8. Geniş alan ağ bağlantı topolojisi 24
Şekil 3.9. Paket filtrelemeli güvenlik duvarı yapısı 26
Şekil 3.10. Uygulama katmanı güvenlik duvarı yapısı 27
Şekil 3.11. Durum denetimli güvenlik duvarı yapısı 28
Şekil 3.12. Uzak erişim sanal özel ağ 29
Şekil 3.13. Siteden siteye sanal özel ağ yapısı 30
Şekil 3.14. Tünelleme 31
Şekil 4.1. Modelleme ve benzetim akış şeması 34
Şekil 4.2. Benzetim ve modelleme araçları sınıflandırılması 35
Şekil 4.3. OPNET modelleme ve benzetim döngüsü 37
Şekil 4.4. Proje düzenleyici 38
Şekil 4.5. Düğüm düzenleyici 39
Şekil 4.6. Süreç düzenleyici 40
Şekil 4.7. OPNET Modeler hiyerarşik modelleme yapısı 41
Şekil 5.1. Kullanılan Modelin Topolojisi 43
Şekil 5.2. “no_firewall_no_vpn” senaryosu 45

Şekil 5.3. Application Config nesnesi uygulama ayarları.....46
Şekil 5. 4. 'Profiles Config' nesnesi profil ayarları 47
Şekil 5.5. İstemci nesnesi profil ayarları.....48
Şekil 5.6. Sunucu nesnesi profil ayarları.....49
Şekil 5.7. rc nesnesi Güvenlik Duvarı Ayarı.....51
Şekil 5.8. "firewall_vpn" senaryosu.....52
Şekil 5.9. 'IP VPN Config' nesnesi ayarları 52
Şekil 5.10. İstatistik verilerini toplama için benzetimin başlangıç ayarları 53
Şekil 5.11. Result Browser penceresi.....53
Şekil 5.12. HTTP sayfası yanıt süresi (saniye) 54
Şekil 5.13. HTTP Alınan Trafik (bayt/saniye).....55
Şekil 5.14. DB Sorgusu Cevap Süresi (saniye).....56
Şekil 5.15. DB Sorgusu Alınan Trafik (bayt/saniye) 57
Şekil 5.16. Eposta İndirme Yanıt Süresi (saniye) 57
Şekil 5.17. Eposta Alınan Trafik (bayt/saniye).....58
Şekil 5.18. internet – ra bağlantı kullanımı (DS1) 59
Şekil 5.19. internet – rb bağlantı kullanımı (DS1).....59
Şekil 5.20. internet – ra bağlantı kullanımı (E1).....599
Şekil 5.21. internet – rb bağlantı kullanımı (E1).....599
Şekil 5.22. Sunucu Yük Performansı (istek/saniye)……..…….60

ÇİZELGELER

Çizelge 5.1. Topolojide Kullanılan Nesneler……..42

Çizelge 5.2. Seçilen İstatistik Verileri…….……..…..48

BÖLÜM 1

GİRİŞ

1.1. Bilgisayar Ağları ve Ağ Güvenliği

İnsanlık tarihi, yaşam tarzını ve hayatı etkileyen farklı çağlardan geçmiştir. Özellikle 1900'lü yıllarda ortaya çıkan teknoloji ürünleri iş ve yaşam hayatını önemli ölçüde etkilemiştir. İş yaşamında kullanılan bilgisayar adı verilen hesaplama işlemlerine yardımcı olan tekil makinelerin yerini kaynaklarını paylaşan makineler almıştır. Bu sistemlere bilgisayar ağı denilmektedir (Tanenbaum & Wetherall, 2011). Birçok bilgisayarı birbirine bağlayarak hem donanımları hem de yazılımları paylaşmak birçok anlamda işlevsellikler sunmaktadır (Alpern & Shimonski, 2010).

İnsanların daha fazla bilgiye ulaşmak istemesi sebebi ile bilgisayar ağları kavramı hayatımızda önemli bir yer tutmaktadır(Sütçü, 2014) . Bilgisayar ağlarının temel amacı bilgiyi paylaşmaktır. Yakın mesafeler ile bu işlem çok problem olmasa bile, uzak sistemlerin birbiriyle iletişim kurması için bir alt yapı gerekmektedir. Bu anlamda internet farklı uzaklıklara dağılmış yapıları birleştiren bir alt yapı olarak tanımlanabilir (Kurose & Ross, 2013). Firmalar, üniversiteler ve devlet kurumlarının hızla büyüyen internet ortamına dahil olmaları çok uzun sürmedi.

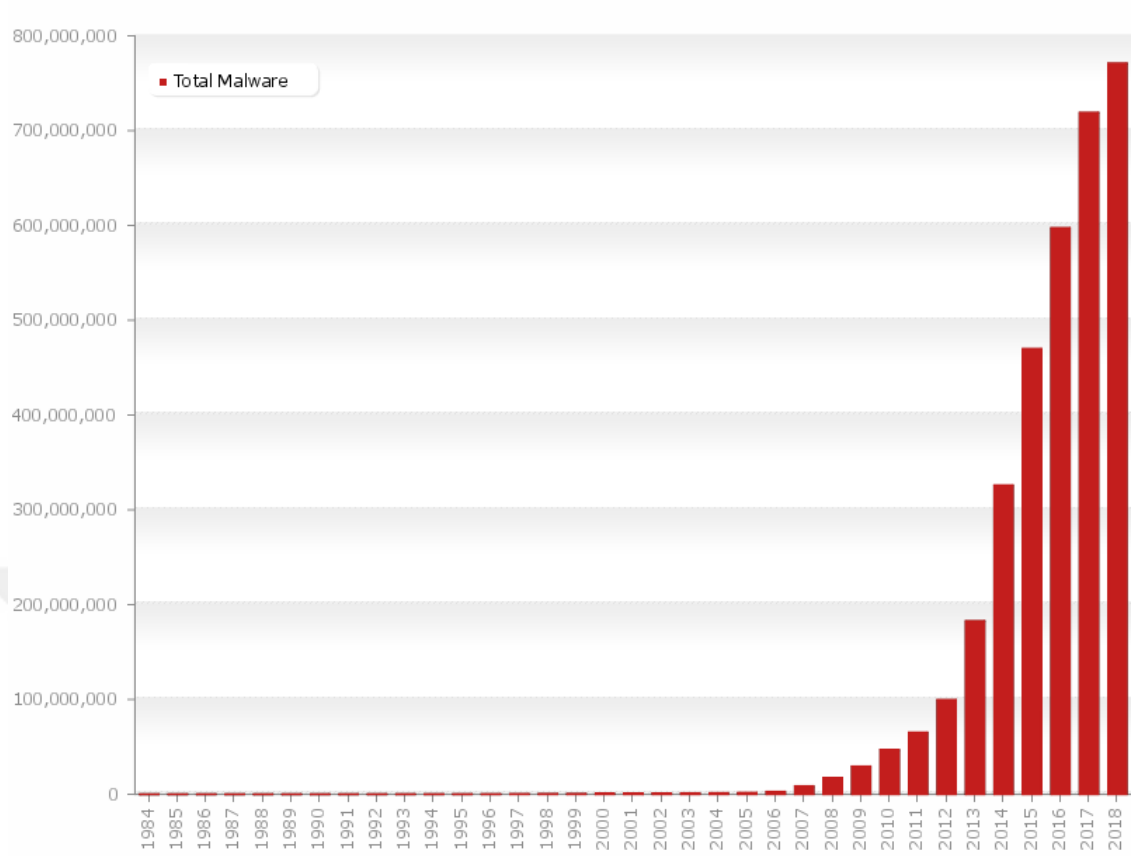
Zaman ilerledikçe bilgisayar ağları ve internet sadece genel bilgileri paylaşmak için değil şirket ve kurumların kişilere hizmet sağladığı bir altyapıya dönüşmüştür. Bu dönüşüm, alt yapıda bulunan güvenlik tedbirlerinin alınmasını veya güncellenmesini gerekli kılmıştır.

Bir bilgisayar ağı dendiğinde akla gelen sorulardan ilki ağın boyutu olacaktır. Aralarındaki mesafeye göre bilgisayar ağları; yerel alan ağı (Local Area Network- LAN) ve geniş alan ağı (Wide Area Network- WAN) adı verilen iki gruba ayrılır. LAN bir bina veya daha dar bir alandaki bilgisayar ağını tanımlarken, WAN ise daha geniş bir alana, bir şehre, bir ülkeye hatta tüm dünyaya yayılmış türdeki bilgisayar ağlarını tanımlamak için kullanılır. Kurumsal uygulamalarda tipik olarak bir çok LAN yapısını WAN yapılarına bağlayan yapılardır (Faircloth, 2014).

Her sistem kullanıldıkça çeşitli avantaj ve dezavantajları ortaya nasıl çıkıyorsa, aynı şekilde iş hayatına dahil edilen bilgisayar ağlarının da başta güvenlik olmak üzere çeşitli sorunları ortaya çıkmıştır. Kişisel bilgilerin korunması, maddi değerlerin sadece bir yerde sanal olarak kayıtlı bilgiler haline gelmesi vb. durumlar; yedekleme, fiziksel güvenlik ve yazılım güvenliği gibi çalışmaların gerekliliğini ortaya çıkarmaktadır.

Büyüyen her yapıda olduğu gibi bilgisayar ağlarının da kontrolü ve yönetilmesi zorlaşır. Bu tür büyük bir ağa sahip kurum ve kuruluşlar ağ yöneticisi adı verilen kişilere ihtiyaç duyarlar. Ağ yöneticisi ağın planlanması, performans yönetimi ve ağın güvenliği gibi değişik görevleri yerine getirir (Alpern & Shimonski, 2010). Ağ güvenliği bu görevler arasında en önemli görevlerden biridir. Ağ güvenliği, bilgisayar ağlarındaki iletilen verinin gizliliğine, bütünlüğüne ve erişilebilirliğine zarar gelmemesi için yapılan eylemlerin tümüdür (Aydın, 2012).

Günümüzde neredeyse tüm kurumlar bilgilerini ve iç yapılarını internet üzerinden erişime açmaktadır. İnternet her yerden ve herkes tarafından ulaşılma gibi fayda ve katkılar sağlasa da, aslında en büyük sorunu da bu sebepten ortaya çıkmaktadır (Fırlar, 2003). Bilişim sistemlerine saldırı amaçlı ortaya çıkan yazılımların Şekil 1.1'de (*Zararlı yazılımların 1984-2018 arası artışı*, 2018) gösterildiği gibi gün geçtikçe artması bilgisayar ağlarının güvenliği konusunu çok önemli bir hale getirmektedir.



Şekil 1.1. Zararlı yazılımların 1984-2018 arası artışı

Bilgisayar ağlarının güvenlik ihtiyacı bir dizi kuralları içeren politikalar ile belirlenir. Burada hazırlanan kurallar Güvenlik Duvarı(Firewall), Sanal Özel Ağlar (Virtual Private Networks- VPN), Antivirüs, saldırı tespit ve önleme sistemleri (Intrusion Detection and Prevention System, IDS/IPS) ve Web filtreleme çözümleri (URL Filtering) gibi yazılım/donanımlarla uygulanabilmektedir (Can & Akbaş, 2014).

1.2. Amaç

Bu tez çalışmasında, sanal özel ağlar ve güvenlik duvarlarının ağ performansına olası etkileri benzetim yoluyla incelenerek, ağ güvenlik yapıları hakkında analizler yapmak amaçlanmıştır. Elde edilen veriler grafik haline getirilerek bilgisayar ağlarındaki güvenlik/performans ihtiyaçlarının daha iyi dengelenebileceği ifade edilmiştir.

OPNET Modeler benzetim yazılımı kullanılarak bilgisayar ağlarının vazgeçilmez iki güvenlik çözümü olan güvenlik duvarları ve sanal özel ağların ağ performansını incelemek amacıyla bir ağ modeli oluşturulmuş ve oluşturulan model üzerinde çeşitli senaryolar uygulanarak elde edilen veriler grafik halinde sunulmuştur. Ağ modelinde

performans incelemesi için üç sunucu ve 800 istemciden oluşan bir istemci/sunucu yapısı oluşturulmuştur. Bu sunucular veri tabanı, web sunucu ve e-posta sunucu olarak yapılandırılmıştır. İstemciler ise sunucuların olduğu uzak ağa ağ trafiği oluşturacak 4 farklı LAN bölgesi şeklinde yapılandırılmıştır.

Oluşturulan ilk senaryoda herhangi bir güvenlik çözümü etkin olmayan "no_firewall_no_vpn" senaryosudur. İkinci senaryoda sistemde bir güvenlik duvarı etkin sanal özel ağ etkin olmayan "firewall_no_vpn" senaryosudur. Üçüncü senaryo ise Güvenlik duvarı ve sanal özel ağın etkin olduğu "firewall_vpn" senaryosudur.

Yapılan çalışmada, literatürdeki çalışmalardan farklı olarak güvenlik uygulamalarının ağ performansına olan etkisi incelenmiştir. Oluşturulan model, senaryolar ve toplanan istatistik verilerin seçimi bu amaca yönelik olarak belirlenmiştir. Bu çalışma, ağ güvenliği ve performansı hakkında çalışma yapmak isteyenler için sıkça kullanılan yöntemlerin, bu iki ihtiyacın da optimizasyonunun sağlanması adına gerekli modelleme ve benzetim yöntemlerinin kullanımını ortaya koymuştur.

1.3. Tez Organizasyonu

Giriş bölümünde bilgisayar ağlarına ve bu yapıların güvenliğine neden ihtiyaç duyulduğu ile çalışmanın amacı anlatılmıştır.

İkinci bölümde; bilgisayar ağı modelleme, ağ performans analizi ve ağ güvenliği çözümlerinin ağ performansına etkileri konusunda yapılan çalışmalar incelenerek bir literatür özeti sunulmuştur.

Üçüncü bölümde, bilgisayar ağları ve ağ güvenliği hakkında genel bilgiler verilmiştir.

Dördüncü bölümde, ağ benzetim yazılımları konusundan bahsedilmiştir. Ayrıca çalışmamızda kullanılan OPNET Modeler yazılımının bir incelemesi yapılmıştır.

Beşinci bölümde, gerçekleştirilen uygulamanın adımları anlatılmış; ortaya çıkan değerler ve grafikler hakkında kısa bilgiler verilmiştir. Bu bölüm çalışmanın Materyal Yöntem bölümünde yer almaktadır.

Altıncı Bölüm, çalışmanın sonuçlar ve tartışma bölümü olup; elde edilen sonuçların anlamları ve katkıları tartışılmış, gelecek çalışmalar için yeni yaklaşımların neler olabileceği ifade edilmiştir.

BÖLÜM 2

LİTERATÜR ÖZETİ

Literatür, modelleme/benzetim yönetimleri ile bilgisayar ağlarının performans incelemeleri ve bilgisayar ağ güvenliği çözümlerinin ağ performansına etkilerinin incelendiği çalışmalar olarak iki farklı başlık altında özetlenmiştir.

2.1. Bilgisayar Ağlarının Benzetim ile Performans İnceleme Çalışmaları

Ahmed, sekiz kolej içeren bir üniversitedeki HTTP, FTP ve E-mail hizmetleri sunan bir bilgisayar ağının modellemesini gerçekleştirmiştir. Çalışmanın ana amacı olarak bilgisayar ağının üç farklı zaman ve yoğunluktaki performans değerlendirmesi olarak belirtmiştir. Ağın en üst seviye kullanım anı ile en az seviyedeki kullanım anında gecikmelerin göz ardı edilecek seviyede olduğunu belirtmiştir. (Ahmed, 2009)

Bıyan ve Alan, Cumhuriyet Üniversitesi ağının, HTTP, E-mail ve Video konferans uygulamaları ile modelleyerek, uzaktan eğitim uygulaması için farklı istemci sayılarında ağ trafiği uygulayarak, ağ performansını incelemiştir. İleriye dönük olarak ağ güncelleme ihtiyaçlarının modelleme ve benzetim yolu ile tespit edilebileceğini belirtmiştir (Bıyan & Alan, 2013). Develi, benzer şekilde Süleyman Demirel Üniversitesi ağını modellemiş ve ağ performansını incelemiştir (Develi, 2009).

Üstündağ, IPv4 ile IPv6 protokolleri yönlendirme performansını uçtan uca gecikme değerlerine göre incelemiş ve IPv6 yönlendirme protokollerinin daha iyi bir başarım elde ettiğini belirtmiştir (Üstündağ, 2009).

Kocabaş, IPv4 ve IPv6 protokollerinin her ikisini de destekleyen yönlendirme protokollerinin performanslarını karşılıklı olarak incelemiş ve IPv6'ya geçiş sürecinde OSPF/OSPFv3 protokolünün en iyi performansı sergilediği sonucuna varmıştır (Kocabaş, 2019).

Khaleel Hasan, OPNET Modeler yazılımını kullanarak, MPLS ve IP yönlendirme gibi iki farlı ağ yapısı kullanarak başarım incelemesi yapmış; MPLS yönlendirmenin daha iyi başarım gösterdiği sonucuna varmıştır. Yine aynı çalışmada WLAN ve WiMAX kablosuz ağ yapılarının performanslarını, QoS tanımlamaları yaparak incelemiş ve Wimax ağının daha iyi başarım gösterdiği sonucuna varmıştır (Khaleel Hasan, 2017). Bir başka çalışmada WiMAX teknolojisi kullanılan ağlarda başarım oranını etkileyen temel faktörler üzerinde durulmuş ve sinyal türüne uygun QoS seçiminin başarıyı arttırdığı belirtilmiştir (Nalbatcı, Bayılmış, İskefiyeli, & Kırbaş, 2013).

Sabit (Fixed) WiMAX QoS'i iyileştirmek amacı ile yeni bir dağıtılmış master-slave modeli önerilmiş ve standart modellere göre daha iyi sonuç elde edildiği benzetim modeli sonuçları ile desteklenmiştir (Lawal, Said, Mu'azu, & Shah, 2014).

Çakır ve Kaptan, VoIP teknolojisine yönelik tehditleri inceleyerek OPNET Modeler yazılımı yardımı ile güvenlik seviyesini yükseltecek unsurlar ortaya koymuşlardır (Çakır & Kaptan, 2009).

Pala, bilgisayar ağlarındaki istenmeyen trafiğin VoIP ses kalitesi ve gecikmesi üzerine etkilerini incelemiş, VoIP trafiğini ayrı bir VLAN üzerinde taşınması durumundaki ses gecikmelerinin kabul edilebilir değerlerde olduğunu, benzetim uygulaması ile elde ettiği verilere dayanarak ifade etmiştir (Pala, 2017).

2.2. Bilgisayar Ağlarındaki Güvenlik Çözümlerinin Benzetim Yolu ile Ağ Performansına Olan etkilerini İnceleyen Çalışmalar

Agbenyegah ve Asante, güvenlik duvarlarının bilgisayar ağlarının performanslarına yönelik etkilerini incelemek için, OPNET Modeler yazılımı ile üç farklı senaryo üzerinde çalışmışlardır. Sonuç olarak internete kaynak paylaşımı yapan her kurumun güvenlik duvarı gereksinimi olduğunu fakat her güvenlik duvarı politikasının ağ performansına olumsuz etkide bulunduğunu belirttikleri çalışmalarında E-mail ve

HTTP uygulamalarının çeşitli ağ parametreleri ile performansını değerlendirmişlerdir (Agbenyegah & Asante, 2017).

Malik ve Verma, IP ağları üzerindeki ses ve video iletişimindeki en çok kullanılan güvenlik çözümü olan VPN yapısının performans incelemesini benzetim yazılımı yardımı ile yapmışlardır. VPN kullanıldığında güvenlik seviyesinin arttığı ancak ağ performansında makul bir düşüş gözlendiğini, bunun da VPN kullanımında gerekli olan şifreleme süreci ve ek kimlik doğrulama başlıklarının neden olduğu sonucuna varmışlardır (Malik & Verma, 2012).

Ahmed ve Nabi Mustafa, VPN üzerinden uzak bir sunucuya bağlanıldığında sunucunun performans etkilerini inceledikleri çalışmalarında bant genişliği ile sunucu işlemci kullanımının ters orantılı değiştiğini gözlemlemişlerdir. Uzun mesafeler arasındaki en güvenli iletişim olan VPN çözümünün ağ performansına olan olumsuz etkilerini azaltmak için daha fazla bant genişliği ve sunucular için daha yüksek teknik özelliklere sahip donanımlar önermişlerdir (Ahmed & Mustafai, 2015).

Zaballos ve arkadaşları, günümüzde ağ güvenliğinin ağ tasarımının öncelikli bir paçası haline geldiğini ve ağ güvenlik testlerinin kolay olmadığını ifade etmişlerdir. Bu noktadan hareketle, benzetim programlarının bize sağladığı yararlardan bahsetmiş ve OPNET Modeler ile eksiksiz bir güvenlik testi yapmak için bir kaynak sunmaya çalışmışlardır. Cisco firmasının önerdiği Cisco Safe modelini referans alarak oluşturdukları test ortamında güvenlik uygulamaları için iki yeni fikir ortaya koyduklarını ifade etmişlerdir (Zaballos, Corral, Serra, & Abella, 2003).

Akbaş ve Gümüşkaya, kurumsal ağlar ile ilgili güvenlik çözümlerinin modellenmesi üzerine yaptıkları çalışmalarında, gerçek bir ağdaki değerler ile OPNET Modeler yazılımından benzetim yolu ile elde edilen değerlerin karşılaştırılmasını yapmışlardır. Çalışmanın bir sonraki aşamasında kurumsal ağ modeli benzetim programı ile modelleyerek, VPN ile güvenlik duvarı çözümlerinin etkin olduğu ve iki güvenlik çözümünün de etkin olmadığı iki farklı senaryo üzerinde incelemeler yapmışlardır. Bu incelemeler sonucunda benzetim araçları ile yapılan ön çalışmaların, bilgisayar ağlarının uygulanması ve ağ güvenlik yapılarının seçilmesi konusunda zaman ve maddi açıdan kazanımlar sağlayacağını belirtmişlerdir (Akbaş & Gümüşkaya, 2011).

Kumar ve Bakon, amaçlarının bilgisayar ağlarında olabilecek güvenlik açıklarının ve güvenlik çözümlerini etkisiz hale getirmek için yapılabilecek saldırıların analizini yapmak olarak açıklamışlardır. Oluşturdukları modeli benzetim yazılımında üç farklı senaryo ile uygulayarak çeşitli ağ metrikleri üzerinden değerlendirmelerde bulunmuşlardır. Her zaman ağların benzetim ortamları ile modellenmesinin gerçek uygulamaya yardımcı olacağını belirtmişlerdir. Sonuç olarak güvenlik çözümlerinin her adımında ağ performansının gecikme oranlarını arttırdığını ifade etmişlerdir (Kumar & Bakon, 2015)

Bu çalışmayı literatürde bulunan çalışmalardan farklı kılan nokta; ağ güvenliği uygulamalarının ağ performansına olası etkilerine odaklanmış olmasıdır. Oluşturulan model ve senaryolardan toplanan istatistiksel veriler bu yönde seçilmiştir. Bu açıdan bakıldığında elde edilen sonuçlar; ağ güvenliği ile ağ performansı arasındaki dengeyi kurmada fikir vereceği düşünülmüştür.

BÖLÜM 3

GENEL BİLGİLER

3.1. Referans Modeller

İnternetin yaygınlaşması ve uzak ağların birbirine bağlanması isteğinin artması ile IP en çok kullanılan protokol haline gelmiştir. IP ile desteklenen bir ağ modeli tasarlanırken referans modeller olan TCP/IP ile OSI arasında olan ilişkinin ve protokollere olan etkilerinin tam olarak bilinmesi gerekmektedir. Amerika Savunma Bakanlığı (DoD) bir ağ modelini 4 katman olacak şekilde modelledi. DoD modeli günümüz bilgisayar ağlarının uçtan uca adresleme yöntemleri, yönlendirme kuralları, hata bulma ve sorun giderme işlemleri için bir açıklama sunmaktadır. Bir ağda ister düğümler arası veriyi fiziksel olarak aktaran ortamlar olsun isterse de işlemleri gerçekleştiren birbirinden bağımsız donanımlar olsun, OSI ve TCP/IP modeline sadık kalmak zorundadır. Günümüzde neredeyse bütün ağ tasarımları hangi kapasitede olursa olsun bu referans modellerin ilkeleri doğrultusunda tasarlanmaktadır. Ayrıca internet üzerinde iletişim tamamen TCP/IP modeli doğrultusunda gerçekleşir (Lloyd, 2001).

Katmanlı bir mimari, her alt birimin kendi İçinde tartışılmasına ve her katmanın gereksiz ayrıntılardan soyutlanmasına izin verir. Bu anlayışla bir katman, altındaki katmandan aldığı hizmetleri işleyebildiği ve üstündeki katmana istediği hizmetleri sunabildiği sürece, herhangi bir katmandaki değişiklik sistemin genelinde bir değişikliğe neden olmaz. Bu sürekli değişen teknolojinin hızlı ve kolay olarak sistemlere uygulanması, katmanlı mimarinin en büyük katkısıdır denilebilir (Kurose & Ross, 2013).

3.1.2. OSI Referans Modeli

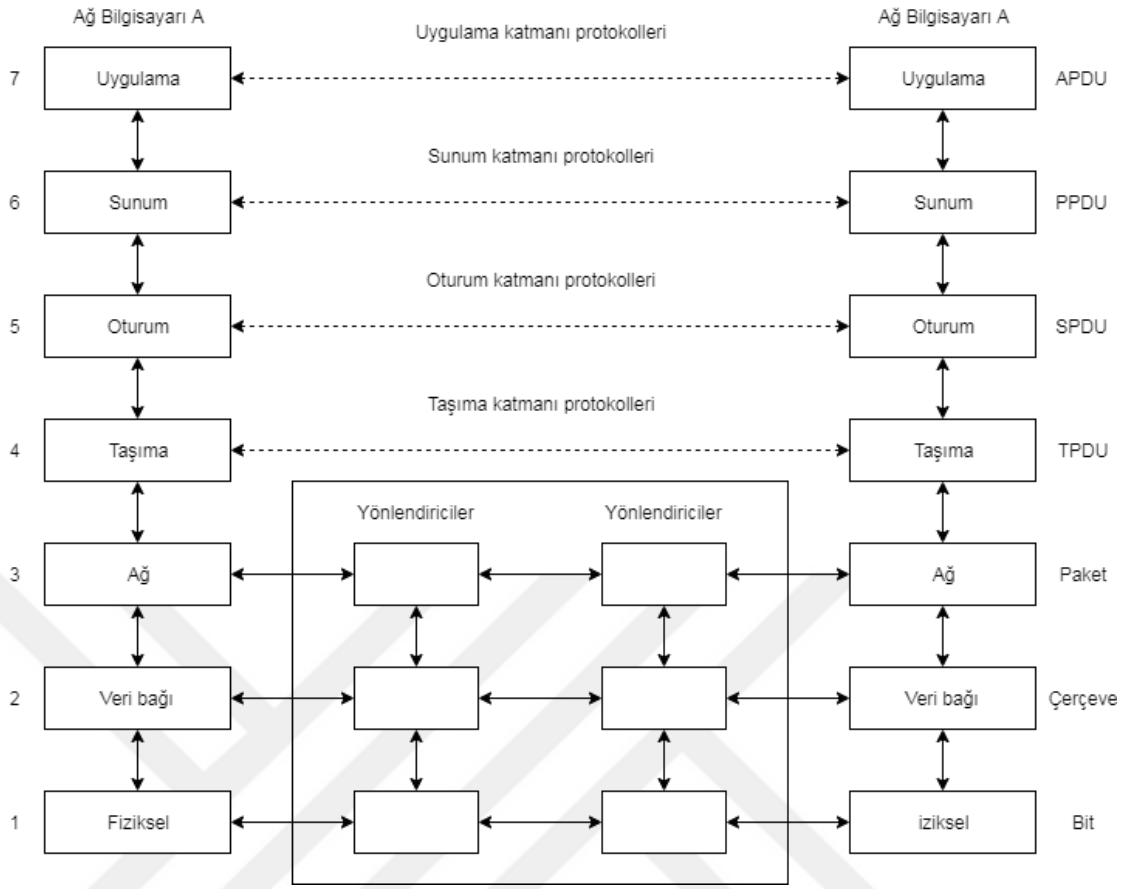
1978'de Uluslararası Standardizasyon Örgütü (ISO) heterojen ağların ortak bir "Açık sistemler Bağlantısı" standardını belirleme için SC16 isimli bir alt komite kurulmasına karar verdi. Görevin büyüklüğü ve teknolojik gerekliliklerin takip edilmesinin zorluğundan dolayı komitenin birkaç alt gruba bölünmesi gerekliydi. Komite, çalışmasının sonunda, tüm ağ geliştiricilerin ihtiyaçlarının en hızlı ve uzlaşmacı şekilde karşılayacak yapının katmanlı bir mimari olacağı kararına vardı (Day & Zimmermann, 1983).

"Açık Sistemler", üretim tarih farklılıkları, yapıları ve karmaşıklık seviyeleri ne olursa olsun, modelde tanımlanan protokollere uydukları sürece, birbirleri ile bağlantı kurma becerisi devam edecek sistemleri ifade etmektedir. OSI soyut bir model olarak, gerçek bir bilgisayar ağını yedi farklı katman kullanarak modeller (Melendez, 1999). Bu katmanlı yapı Şekil 3.1' ifade edildiği gibidir.

1. Fiziksel Katman: Bu katmanın görevi bitleri sinyallere dönüştürmektir. Birden fazla kullanıcının aynı iletim ortamını kullanmasını sağlamak için sinyalde gerekli düzenlemeleri yapar. Uçtan uca veri aktarılırken her ortama uygun elektrik sinyallerinin dönüşümlerini yapar.

Bu katman daha çok mekanik ve elektriksel işlevsellikler ile ilgilenir. Kablolama, pin yapısı, bağlayıcı tasarımları ve hub, tekrarlayıcı cihazları gibi belirlemeler bu katmanın içeriğindedir (Madan & Bharti, 2014). EIA / TIA RS-232, EIA / TIA RS-449, V.35, RJ-45 gibi iletim ortamı için gerekli olan özellikler bu katmanda belirlenir (Li, Li, Cui, & Zhang, 2011).

2. Veri bağı katmanı: genel olarak ağ cihazları arasında veri aktarmak ve fiziksel katmandaki oluşabilecek hataları tespit etmek bu katmanın görevidir. Senkronizasyon, hata ve akış kontrolü tipik olarak bu katmanın görevidir (Melendez, 1999). NIC, Ethernet ve jetonlu halka ağ anahtarları ile köprüler bu katmanda çalışırlar (Madan & Bharti, 2014). Döngüsel artıklık kontrolü (CRC), SDLC, HDLC, PPP, STP, Frame Relay gibi işlem ve protokoller bu katman dahilindedir (Li vd., 2011).



Şekil 3.1. Yedi katmanlı OSI mimarisi

3. Ağ katmanı: Bu katmanın ana işlevi mantıksal adresleme yapmak ve iletişimin sağlanacağı yönü tayin etmektir. Bu katmanda kullanılan IP adresi alt ağ adı verilen küçük parçalara bölünerek, yönetimi kolaylaştırır ve verilerin ağlar arasında yönlendirici adı verilen cihazlar sayesinde kolayca iletilmesini sağlar (Madan & Bharti, 2014). Bu katman IP, IPX, RIP, OSPF vb. protokolleri barındırmaktadır (Li vd., 2011).

4. Taşıma Katmanı: Uçtan uca bilgisayarlar arasında bağlantı bu katmanda sağlanır. Bu katmanda farklı cihazların iletişim kurması sağlanır. Taşıma katmanındaki veri biriminin adı TPDU'dur. İletilen mesajın boyu büyük ise bu katman mesajı segment adı verilen bölümlere ayırır ve birleştirir. Bağlantı kontrolü, teslimat kontrolü ve iki uç düğüm arasında hangi uygulamalar üzerinden işlem yapılacağı bu katmanda belirtilir. Uygulamalar için port adresleme bilgilerini belirlemek bu katmanın görevleridir (Madan & Bharti, 2014).

5. Oturum katmanı: İki bilgisayar arasında iletişimi başlatmak ve kontrol etmek için bir oturum oluşturur. İki sunum oturumu arasındaki işlevselliği sağlamak için oturum

yönetimi işlemleri ve oturum diyalog işlemlerini yürütür (Zimmermann, 1980). Oturum katmanında veri senkronizasyonunu sağlamak için verilere kontrol noktaları eklenir. Oturum katmanı farklı cihaz ve makineler ile iletişimi sağlar (Li vd., 2011).

6. Sunum katmanı: Veri kaynağından gelen verinin tipini (ASCII, GIF, MPEG vb.) anlamak ve iletişimdeki sistem şifresi gibi verilerin şifresini çözmek, formatlar arası dönüşüm yapmak ve veri sıkıştırmak/açmak bu katmanın görevidir. Veri iletiminde kullanılan veri tiplerini anlamak, standardize hale getirmek kaynak ve hedef arasındaki en büyük sorunlardan biridir. Bu sorunun çözümü tipik olarak yine bu katmanın görevidir (Li vd., 2011).

7. Uygulama Katmanı: Kullanıcının etkileşimde olduğu katmandır. Son kullanıcı işlemlerinin desteklendiği, kullanıcı doğrulama, gizlilik ve söz dizimi gibi konuların ele alındığı katmandır. Bu katman dahilinde DNS, NFS, POP3, SMTP, HTTP, HTTPS, FTP, SSH vb. birçok protokol ve uygulama bulunur.

3.1.3. TCP/IP Referans Modeli

1960'larda bilgisayarları birbirine bağlamanın ve kaynakları paylaşmanın sağlayacağı avantajların daha farkına varılmamıştı. Birçok donanım üreticisi vardı ve donanımlar arası uyum sorunları mevcuttu. Firmalar bilgisayar ağları kullansalar da bu ağlar genelde yerel alan ağları idi. Bu işlemler için hızlı kurulum ihtiyacı daha fazlaydı. Bu ihtiyacı da Novell Netware firmasının IPX/SPX protokol yığınları çok daha iyi sağlamaktaydı. Amerikan Savunma Bakanlığı uzak mesafelerdeki tesislerin aralarında iletişim kurmanın gerekliliğini fark etti. Bu projeye Amerika'daki büyük üniversiteler de destek oldular. Gelişmiş Araştırmalar Projeleri Ajansı (ARPA) 1968 yılında böyle bir ağ için girişimlere başladı. 1969 yılında ARPAnet'in ilk düğüm veya bağlantı noktası Los Angeles'taki California Üniversitesi'nde kurulmuş oldu (L. Shinder, 2000). İlk sunulan protokol paketi farklı ağlarda istenilen düzeyde çalışmaya uygun olmayınca TCP/IP protokol paketinin ortaya çıkmasına neden olan süreç başlamış oldu (Cerf & Kahn, 1974). Cerf ve Kahn 1970'lerin başında Ağ Geçidi fikrini ortaya atarak şu anda internet ile kullanılan TCP/IP protokol paketinin ilk özelliklerini yazdılar (Gallo & Hancock, 2002b).

TCP/IP protokol takımı tam olarak açıklaması RFC-1180 de yapıldığı gibi dört katmandan oluşmaktadır (Kale & Socolofsky, 1991) . Bu katmanlar sırasıyla:

- Uygulama Katmanı
- Konakçı Bilgisayar-Konakçı Bilgisayar arası taşıma katmanı
- İnternet katmanı
- Ağ arayüz katmanı

katmanlarıdır. Şekil 3.2'de TCP/IP ile OSI katmanları karşılaştırmalı bir biçimde gösterilmiştir.

<table>
<tr><th></th><th>OSI Katmanları</th><th colspan="2">Protokoller</th><th>TCP/IP Katmanları</th></tr>
<tr><td>7</td><td>Uygulama</td><td rowspan="3">SNMP
TFTP
NFS
DNS
BOOTP</td><td rowspan="3">FTP
Telnet
Finger
SMTP
POP</td><td rowspan="3">Uygulama</td></tr>
<tr><td>6</td><td>Sunum</td></tr>
<tr><td>5</td><td>Oturum</td></tr>
<tr><td>4</td><td>Taşıma</td><td>UDP</td><td>TCP</td><td>Konakçı Bilgisayar-Konakçı Bilgisayar arası taşıma katmanı</td></tr>
<tr><td>3</td><td>Ağ</td><td colspan="2">IP</td><td>İnternet</td></tr>
<tr><td>2</td><td>Veri bağı</td><td colspan="2">Ağ arayüz kartları</td><td rowspan="2">Ağ arayüz</td></tr>
<tr><td>1</td><td>Fiziksel</td><td colspan="2">Fiziksel iletim ortamı</td></tr>
</table>

Şekil 3.2. TCP/IP ve OSI katmanları karşılaştırması.

Uygulama Katmanı: Bu katman protokollerinin birkaçı OSI katmanına denk gelir. OSI de bulunan oturum, sunum ve uygulama katmanları, TCP/IP de tek bir katmana indirgenmiştir. Sunum katmanının görevlerini SSL ve S/MINE protokolleri üstlenir. Bu katmanda protokoller kullanım amaçlarına ve yapılarına göre iki grupta ifade edilebilir. Kullanıcı protokolleri: Kullanıcı uygulamaları tarafından kullanılan; HTTP, SMTP,

Telnet, FTP, IMAP ve DNS gibi protokoller. Hizmet protokolleri, İnternet kullanıcılarının pek karşılaşmadıkları, fakat ağ yapılarının doğru çalışıp çalışmadığını test etmek için ağ uzmanları tarafından kullanılan protokolleridir. Bunlara en iyi örnek, ağ cihazlarının yönetiminde kullanılan SNMP'dir (Dostálek & Kabelová, 2006).

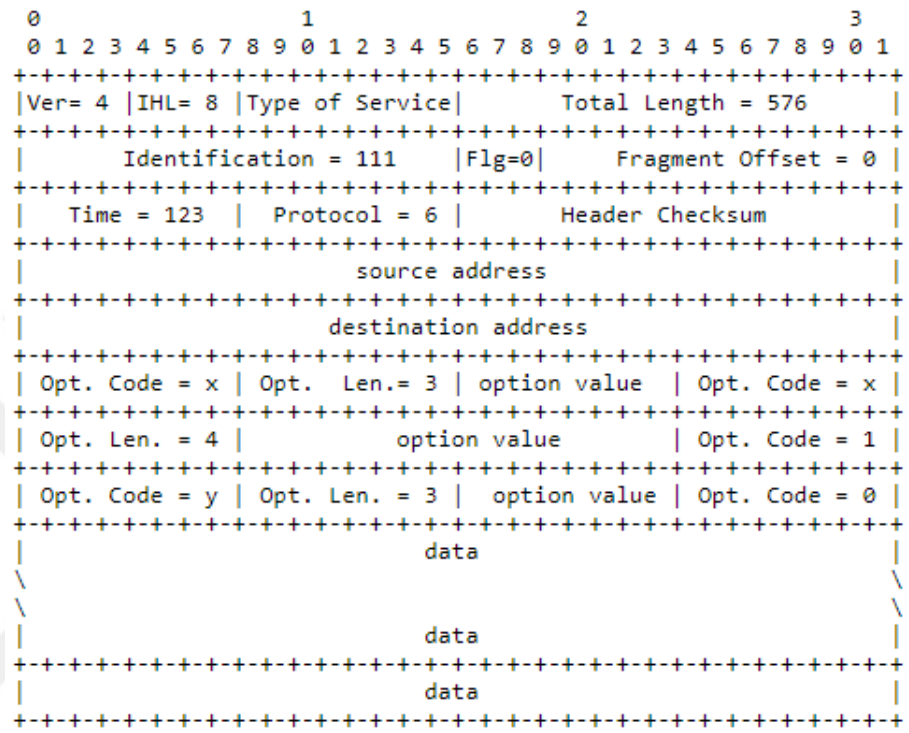
Taşıma Katmanı: Bu katman TCP ve UDP gibi temelde iki protokol içermektedir. Bu iki farklı protokolün tanımını şöyle yapabiliriz (Goralski, 2017b):

- TCP iletişim esnasında bozulan veya kaybolan segmentlerin gönderimini tekrar sağladığı için güvenli bir protokoldür. TCP protokolünün, ses ve video gibi anlık veri iletimi isteyen ve gecikmeye karşı duyarlı iletişim türlerinin üzerinde olumsuz etkileri vardır. Bu anlamda anlık iletişimde kullanılması tavsiye edilmez. TCP bağlantısız çalışan internet katmanı protokolü IP üzerinde bulunarak; bağlantılı iletişimin yönetimini devralır.
- UDP protokolü ise IP protokolü için bağlantısız bir yönetim sunar. Bu anlamda ses ve video iletişimi gibi anlık iletişimler için tercih edilir. UDP, segmentlerin bir şekilde hedefe ulaştığını varsayar.

İnternet katmanı: Bu katman IPv4, ICMP, ARP, IPv6 ve yönlendirme protokolleri gibi önemli protokolleri barındırmaktadır (Mackay, Wright, Reynders, & Park, 2004) :

- IPv4 uç cihazlar arasındaki paketlerin dağıtımından sorumludur. Bir posta sistemine benzer şekilde paketlerin hat boyunca belirtilen adreslerde en iyi yoldan yolculuk etmesini sağlar. Bu iş 32 bitlik hem kaynak hem de hedef adresi bildiren adres bilgilerini kullanır. IP farklı boyuttaki paketleri parçalamak zorundadır. Örneğin; Ethernet 1500 bayt taşıyabilirken içerirken X.25 ise 576 bayt veri taşıyabilmektedir. Bu anlamda her IPv4 paketi kaynaktan çıktıktan sonra parçalanabilir; fakat aynı şekilde hedefte tekrar inşa edilir. Şekil 3.3 RFC 791'de tanımlandığı şekli ile örnek IP paketi ve bölümleri göstermektedir. IP adreslerinin küresel olarak dağıtımından sorumlu kuruluş İnternet Atanmış Numaralar Otoritesi IANA'dır. IANA, IP adreslerini Bölgesel İnternet Kayıtçılarına (RIR) verir, bu kurumlarda bu numaraları İnternet Servis Sağlayıcılarına (İSS) son kullanıcılara veya diğer İSS'lere satmaları için verir. IPv4 "11000000 10101000 00010110 00000001" gibi 32 bitten oluşmaktadır. Bu yapının insanlar tarafında

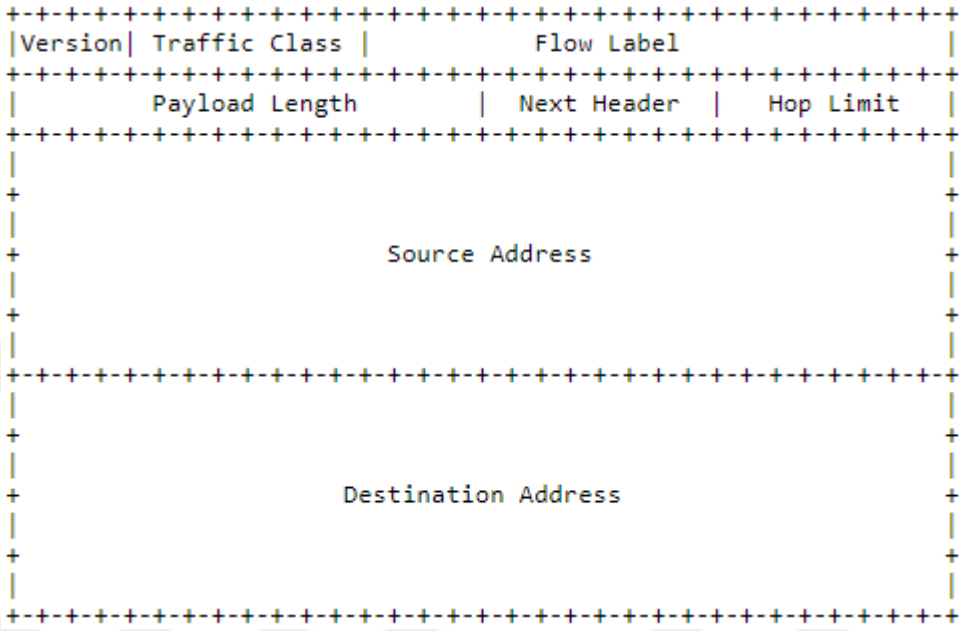
okunması zor olduğu için; “192.168.22.1” şeklinde her 8 bitin 0-255 arası onluk sayı sistemi ile yazılması ile ifade edilir. IPv4 Adresi uç cihazın hangi ağa dahil olduğunu gösteren “ağ kimliği” ve ağdaki hangi bilgisayar olduğunu belirten “cihaz kimliği” gibi 2 kısımdan oluşur (Postel & Reynolds, 1983).



Şekil 3.3. Örnek IPv4 paketi (Postel, 1981b).

- ARP (Address Resolution Protocol): Ethernet ağında donanım adresi olarak kullanılan MAC adresleri ile IPv4 adresleri arasında herhangi bir ilişki kurulamaz. Bu durumda iletişim için gerekli olan donanım adresinin elde edilmesi zorlaşır. ARP, bu ve benzeri donanım adresi ile ilgili sorunların üstesinden gelmek için tasarlanmış bir protokoldür (Plummer, 1982).
- ICMP (Internet Control Message Protocol): Düğümler arasında iletişimde gecikmeler veya problemler yaşandığında, ICMP yapısı bu sorunların çözümü için bir ileti ile raporlama yapar. IP güvenilir iletişim sağlayacak şekilde tasarlanmamıştır. Bu kontrol protokolünün temel amacı; IP paketlerinin iletiminde doğacak sorunları rapor etmektir (Postel, 1981a).
- IPv6: Dünya üzerinde internete ulaşmak isteyen kişilerin sayısının artması ve IPv4’te çeşitli açıkların ortaya çıkması ile hem 32 bitlik adres yapısı yetersiz oluşu

hem de yeni güvenlik sorunları yeni bir protokol ihtiyacını ortaya çıkarmıştır (Kartal, Sağiroğlu, & Bülbül, 2013). Bunun gibi sorunların aşılması için arttırılan adres kapasitesi ile beraber, güvenilir ve basitleştirilmiş adresleme yapısına sahip IPv6 protokolü ortaya çıkarılmıştır (Durkaya, Bascil, & Er, 2011). Basitleştirilmiş başlık formatı (RFC 2460) Şekil 3.4'te gösterildiği gibidir.



Şekil 3.4. IPv6 başlık biçimi

- Yönlendirme: İnternet katmanının temel görevlerinden biri de iletişimi bir uçtan diğer uca ulaşacak şekilde paketleri bir sonraki düğüme ulaştırmaktır. IP ağında hiçbir düğüm yani yönlendirici gidilecek hedef hakkında tam bir bilgiye sahip değildir. Bu işlemi gerçekleştirmek için her yönlendirici görevi gören cihaz kendine gelen paketleri hedefine ulaştırmak için ya sabit olarak ayarlanmış bir sonraki yönlendiriciye ya da yönlendirme protokolleri ile otomatik olarak öğrenilmiş yönlendiriciye iletir. Her yönlendirici sadece aynı yönlendirme otonom sisteminde olan yönlendiriciler tanır (Reynders, Mackay, Wright, & Mackay, 2004).

Ağ arayüz katmanı: Bu katman modeldeki en düşük katman olmakla beraber, bağlantı katmanı; seri hatlar ve Ethernet gibi bağlantıların internet katmanına destek ve hizmet sunması işlemini sağlamaktadır (Tanenbaum & Wetherall, 2011).

3.2. Ağ Yapıları

Bir ağ alt yapısı oluşturmak ve bunu internet gibi bir WAN üzerinde kurumun ihtiyaçları doğrultusunda tasarlamak iyi düzeyde planlama, zaman ve maddi yatırım yapmak demektir. Bir kurum ağ alt yapısını kullanarak ister küçük bir alanda ister uzak alandaki şubeleri ile iletişim haline geçmeyi planlıyorsa bu; hem çok fazla ve farklı üretici hem de çok farklı protokollerin beraber çalışabilmesi anlamına gelmektedir. Bu işlemi gerçekleştirmek için en uygun ağ topolojilerinin, ağ yönlendirme ve ağ anahtarlaması protokollerinin belirli bir tasarım mantığı ile oluşturulması gerekmektedir. Şu başlıklara dikkat etmek işimizi kolaylaştıracaktır: Hiyerarşi tasarımı, topoloji tasarımı, protokol seçimi ve yönlendirme algoritmalarının baştan planlanması (Kenyon, 2002).

3.2.1. Mantıksal Ağ Topolojileri

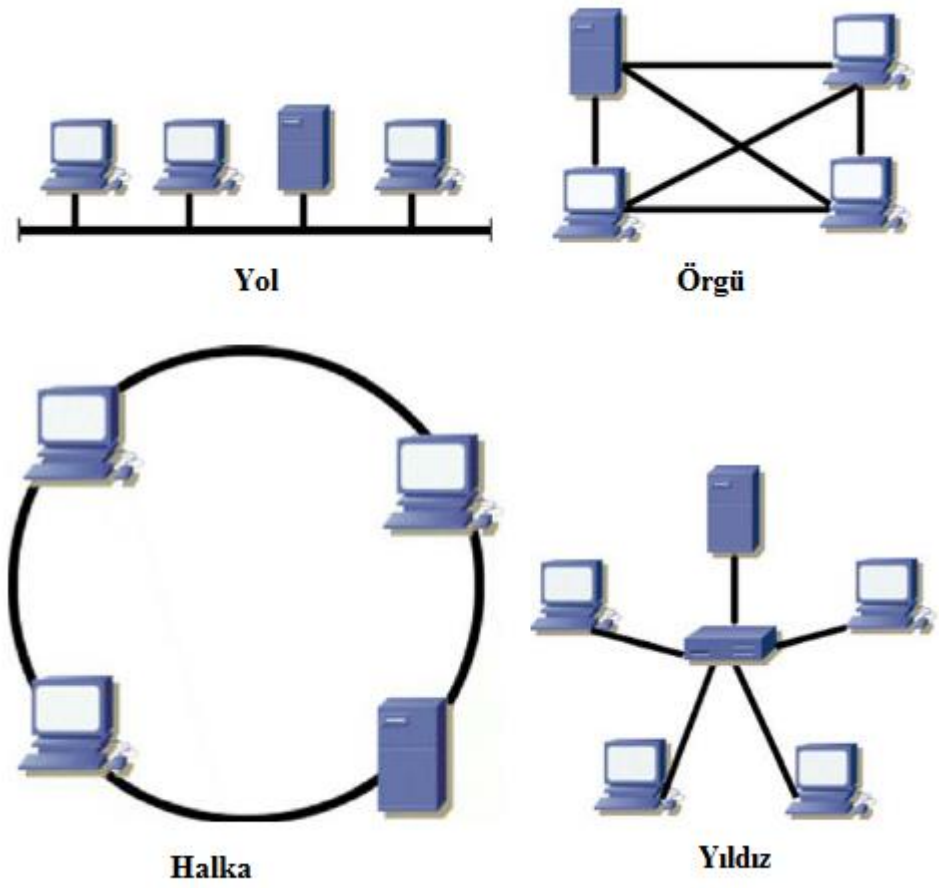
Bir kurumsal ağ yapılandırılırken seçilebilecek mantıksal topoloji ve modeller şunlar olabilir (Alpern & Shimonski, 2010) :

- **Merkezi (Centralized):** Bu ağ modelinde kaynaklar merkezi bir noktaya konumlandırılır ve yönetilir. Bu yönetmede bir ağ yöneticisi kaynakları daha kolay yönetebilir. Örneğin verilerin bulunduğu sabit diskler veya merkezi bir yazıcının yönetimi çok daha kolay hale gelir.
- **Merkezi olmayan, dağıtılmış (Decentralized-distributed):** Ağın kaynakları farklı bölgelere dağılmış şekilde bulunur. Bu alanlardaki sistem yöneticilerine yerel yetkiler ve sorumluluklar atanarak, kaynak yönetimi sağlanabilir. Çok farklı yerlerde hizmetler sunan kurumlar için, ağ kaynaklarının dağıtılması performans ve yönetilebilirlik açısında olumlu etkiler sunar. Bu durum uzak sunuculara sürekli WAN üzerinden ulaşmaya çalışan merkezileşmeye göre daha iyi bir ağ başarımı demektir.
- **Eşler arası (Peer-to-peer):** Her iş istasyonunun eşit olduğu ve kaynaklara eşit yetkilerle ulaşabildiği bir ağ modelidir. Her iş istasyonu/bilgisayar diğer bilgisayarların ulaşım bilgilerini bilmek zorundadır. Her bilgisayar, ağdaki hesap ve kullanıcı bilgilerini kayıt altında tutmak zorundadır. Kurulması ve küçük alandaki ağlar için uygulaması kolay olan bir ağ türüdür. Bu anlamda iş istasyonu sayısı arttıkça yönetimi zorlaşır.

- **İstemci/sunucu (Client/Server):** Eşler arası ağda her iş istasyonu iletişimin yönüne göre hizmet alan veya hizmet eden rolünü alabilir. Bu ağ modelinde ise ağa bağlı cihazlar arasında hizmet eden ve hizmet alan gibi bir ayrım vardır. Bu modelde hizmet alan rolündeki istemciler veri ve ağ kaynaklarını kendi İçinde barındırmazken, hizmet veren rolündeki sunucular ise ağ kaynaklarını ve ağda bulunan verilere ulaşmak isteyen diğer cihazların yetkilerini belirleyen bilgisayarlardır. Her sunucu bilgisayar belirli bir ağ kaynak rolünü istemcilere sunmak için özelleştirilebilir.
- **Sanal Özel Ağlar (VPN):** İnternet gibi ortak bir ağ yapısını kullanarak, uzak ağlar ile güvenilir bağlantılar yapmayı sağlayan ağ teknolojisidir. Çoğu durumlara hem güvenlik hem de kurumdaki ağ kaynaklarına istenilen yerde ulaşılmasını sağlayan ve bazen de kuruluşlara ait küçük şubelere atanmış bağlanmayı özel bağlantılardan çok daha az maliyetle çözebilmesinden dolayı çokça tercih edilen bir teknolojidir. İki farklı yerdeki ağları birbirine bağlayan (site-to-site) ve uzak bir ağ kaynağını erişimi (remote access) gibi iki tipi mevcuttur.
- **Sanal Yerel Alan Ağı (VLAN):** Yerel alan ağlarının, aynı ağ anahtarlama cihazları ve yönlendiriciler ile mantıksal alt ağlara bölünmesini sağlayan yapılardır. Böylelikle cihazlar aynı ağ anahtarına bağlı olmalarına rağmen mantıksal olarak değişik alt ağlarda bulunacaklardır. Bu durumda ağ yönetimi ve donanım maliyetleri daha kabul edilebilir seviyelerde olacaktır.

3.2.2. Fiziksel Ağ Modelleri

Fiziksel ağ modelleri; ağ cihazlarının konumu, ağ kablolarının düzeni ve ağın nasıl yapılandırıldığı ile ilgilenir. Bu ağ modelleri tek başına kullanılabileceği gibi birkaçının ortak kullanımı da mümkündür (Alpern & Shimonski, 2010). Şekil 3.5'te birkaç fiziksel ağ topolojisi gösterilmektedir.



Şekil 3.5. Fiziksel ağ topoloji örnekleri

Bu fiziksel topoloji ve modelleri aşağıdaki gibi ifade edebiliriz (Comer, 2009):

- **Yol (Bus):** Bu topolojide bütün cihazlar tek bir hattan oluşan bir koaksiyel kabloya bağlıdır. Hat sonunu belli etmek için hat sonlandırıcılar kullanılır. Hat üzerinden iletilen veri tüm bilgisayarlara iletilir, veri hangi hedef bilgisayarı adreslemiş ise o bilgisayar veriyi alır. Kablo yapısı güvenilir olsa da ağa yeni bilgisayar eklemek zordur. Mesafe ve ağa katılabilecek bilgisayar sınırlılıkları vardır.
- **Yıldız (Star):** Her ağ bilgisayarı, birbirine veya bir kabloya değil merkezde bulunan bir ağ anahtarına veya hub cihazına bağlıdır. Hattaki bir kablonun arızası sadece ilgili bilgisayarda sorun çıkarır. Merkezi cihazda çıkan sorun bütün ağın iletişimini durdurur. Ağ genişlemesi ve arıza takibi kolaydır.
- **Halka (Ring):** Her bilgisayar eğer ağda iletilen veri varsa, veriyi hedefe ulaştırana kadar bir sonraki bilgisayara iletir. Ağ dairesel olarak devam ettiği için bir kablo

sonlandırıcıya ihtiyaç yoktur. Halka da bilgi akışı tek yönlüdür. Bundan dolayı ağda arızalanan bir kablo veya bilgisayar ağ iletişiminin kesilmesine neden olur. Ağ yapısı genişlemeye ve arıza bakımına uygun değildir.

- **Örgü (Mesh):** Arızaya ve hataya en toleranslı fiziksel ağ modelidir. Her bilgisayar ile diğer bilgisayarlar arasında bir hat mevcuttur. Bu şekilde ağdaki bilgisayar veya kablolama arızaları diğer modellere göre daha az probleme sebep olur. Hataya ve anlık iletişim kaybına tahammülü olmayan işletmelerde sıklıkla tercih edilir.
- **Noktadan Noktaya (Point-to-point):** İki ağ düğümünü birbirine özel olarak bağlayan sürekli, kalıcı ve güvenilir ağ ihtiyaçlarını karşılayan bir yapıdır. Genelde iki farklı alandaki şubeleri merkeze veya birbirine güvenli biçimde bağlayan bağlantı türüdür. T1 ve DS1 hatları bu topolojinin en bilinen örnekleridir.
- **Noktadan Çok Noktaya (Point-to-multipoint):** İkiden fazla ağ düğümünün bağlandığı, donanım ve yazılım ihtiyacına göre katlanarak büyüyen bir ağ topolojisidir. Bu topolojide genelde bir düğüm ana merkez konumunda olur ve diğer düğümler ana merkeze erişmeye çalışan şubeler konumundadır. Asenkron aktarım modu (ATM) ve çerçeve aktarma (Frame Relay) bu topolojinin en iyi bilinen örnekleridir.

3.2.3. Coğrafi Kapsamlarına Göre Ağ Türleri

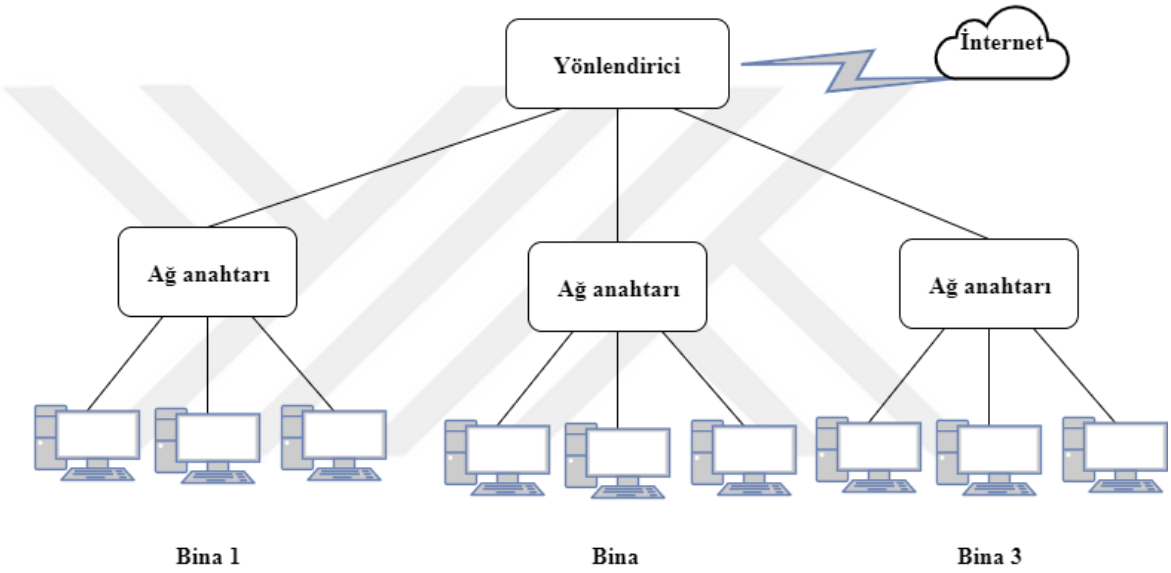
Çoğu zaman bilgisayar ağları, uç cihazlar arasındaki mesafelere göre sınıflandırılır. Bir bina ya da bir kurumun binaları arasındaki ağa yerel alan ağı (LAN) denir. LAN IEEE tarafından genellikle 10 kilometreden az çaptaki bir alana yayılmış bilgisayar ağları için kullanılır. Daha geniş alanda bir ağ iletişimi var ise bu ağlara; geniş alan ağları (WAN) adı verilir. WAN IEEE tarafından, genellikle 100 kilometre çapından daha geniş alanlara yayılmış ağları ifade etmek için kullanılır. WAN coğrafi olarak ülkeler hatta kıtalar arası ağları tanımlamak için kullanılır (Gallo & Hancock, 2002a).

Coğrafi kapsamlarına göre ağlar genelde şu sınıflar altında incelenebilir (Alpern & Shimonski, 2010): Yerel alan ağı (Local area network-LAN), geniş alan ağı (Wide area network - WAN), şehir alan ağı (Metropolitan area network - MAN), depolama alan

ağı (Storage area network - SAN), kişisel alan ağı (Personal area network - PAN), kampus alan ağı (Campus area network - CAN).

PAN, günümüzde evlerdeki bilgisayarların birbirine bağlanması ihtiyacı veya mobil cihazların birbirleri ile iletişim kurma ihtiyacı için kullanılan ağlardır. MAN, LAN yapılarından büyük fakat WAN yapılarından küçük şehirsel ağları ifade eden yapılardır. SAN, veri depolama işlemini yönetilebilir ve daha başarılı hale getirmek için oluşturulmuş hızlı bağlantıları olan depolama aygıtlarından oluşan bir ağ yapısıdır.

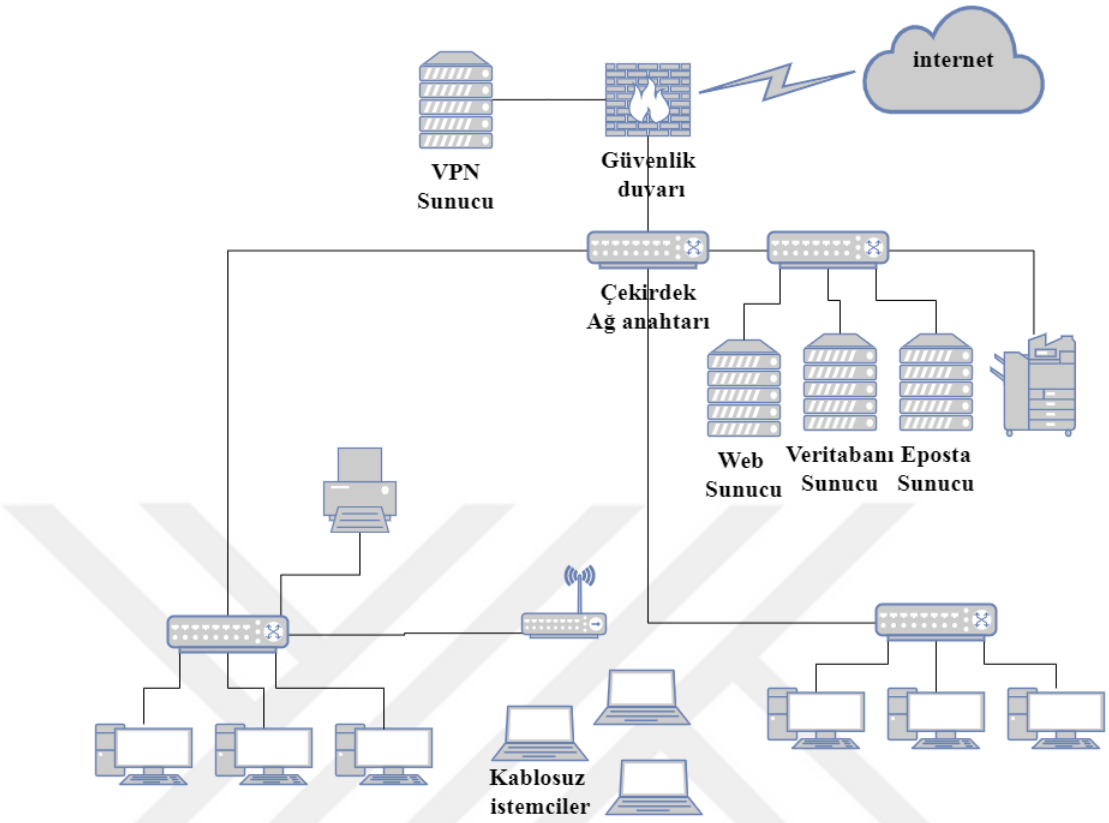
Şekil 3.6'da örnek bir yerel alan ağı yapılandırılması verilmiştir.



Şekil 3.6. Örnek yerel alan ağı

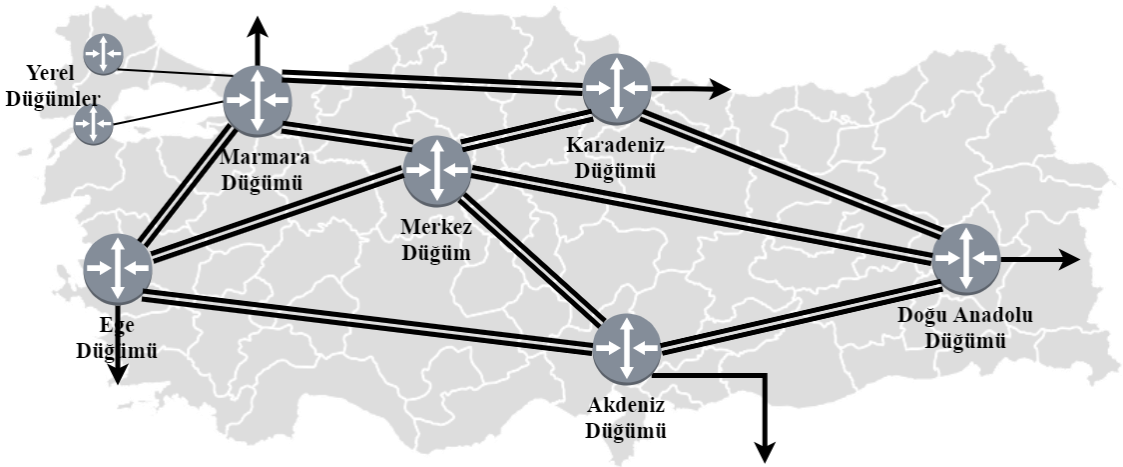
3.2.4. Kurumsal Ağlar

Kurumsal ağlar temel olarak Şekil 3.7'de olduğu gibi tanımlanabilir. İster bir üniversite isterse belli bir bina veya alandaki kurumlar olsun, günümüzdeki kurumsal ağ yapısı örnekleri büyük oranda bu şekildedir. Çalışan veya müşterilerine dahili ağdaki kaynakları güvenli olarak genel ağ üzerinde paylaşmayı sağlayan VPN, dahili ağa gelen bağlantıları kontrol ederek istenmeyen iletişimleri engelleyen güvenlik duvarı, ağ kaynaklarını paylaşmayı ve yönetimini kolaylaştıran sunucular, kablolama olmaksızın ağa erişmeyi sağlayan kablosuz ağlar, neredeyse günümüzde her orta ve büyük ölçekteki kurumun temel ihtiyaçları haline geldi (Hofmann & Beaumont, 2005). Bu tür bir yerel ağ çözümü hem güvenlik ihtiyaçlarını hem de genişlemeye yönelik ihtiyaçları karşılayabilecek niteliktedir.



Şekil 3.7. Kurumsal ağ yapısı örneği

Kurumsal ağların ihtiyaçları daha büyük bir ölçekte dağıtılmış bir yapı gerektirebilir. Bu tür durumlarda geniş alanlardaki şube ve tüketicilere ulaşmak için kurumsal bir ağ Şekil 3.8'deki belirtildiği gibi yapılandırılabilir. Geniş alan ağları internet servis sağlayıcıları (İSS) tarafından sağlanan ağ alt yapısı ve cihazlar ile yapılandırılabilmektedir. Bu yapı ile genişleme sağlanarak kurumların bir ülke, kıta hatta küresel çapta olan istekleri karşılanmış olur (Hofmann & Beaumont, 2005).



Şekil 3.8. Geniş alan ağ bağlantı topolojisi

3.3. Ağ Güvenliği

Günümüzde çoğu bilgisayar ağı internet adı verilen genel ağa bağlı durumdadır. Bu sebepten bilgisayar ağ alt yapılarının güvenlik önlemlerinin doğru yapılandırıldığından emin olmak çok önemlidir. Güvenlik ağ uzmanlarının ağa yetkisiz girişleri ve saldırıları tespit edecek şekilde; gerekli yazılım ve donanımları kullanabilmeleri gereklidir. Sunulan hizmetleri kullanacak kişi veya cihazların ağ kaynaklarını hangi yetkilerle, nasıl kullanılacağı tespit edilmeli ve aksaklıklara yol açmayacak şekilde güvenlik çözümleri uygulanmalıdır. Etkin bir biçimde veya hiç kullanılmayan hizmetler her zaman ağda bir saldırı noktası olarak kullanılabilir. Etkin kullanılmayan hizmetlerin tespit edilmesi ve gerek görülürse devre dışı bırakılması, daha temiz ve saldırılara karşı daha güvenli bir ağ yapısı ortaya çıkaracaktır. Güvenlik sorunu yaşayan bilgisayar ağlarının birçoğunun problemi tasarımda bulunan eksiklik veya yanlışlıklardan dolayı ortaya çıkmaktadır (Dubrawsky, 2010).

3.4. Güvenlik Duvarları

Güvenlik duvarları binalardaki gerçek duvarlara çok benzer; ana amaç duvarın diğer tarafında olan kötü etkiler oluşturabilecek bir durumu engellemektir (Krit & Haimoud, 2017). Güvenlik duvarının temel amacı; dahil olduğu ağa dış ortamdan gelecek erişim isteklerine bir engel oluşturarak bu istekleri değerlendirmektir. Bu nedenle iç ağımıza dışarıdan gelecek erişim isteklerine cevap verme işlemi merkezileştirilmiş

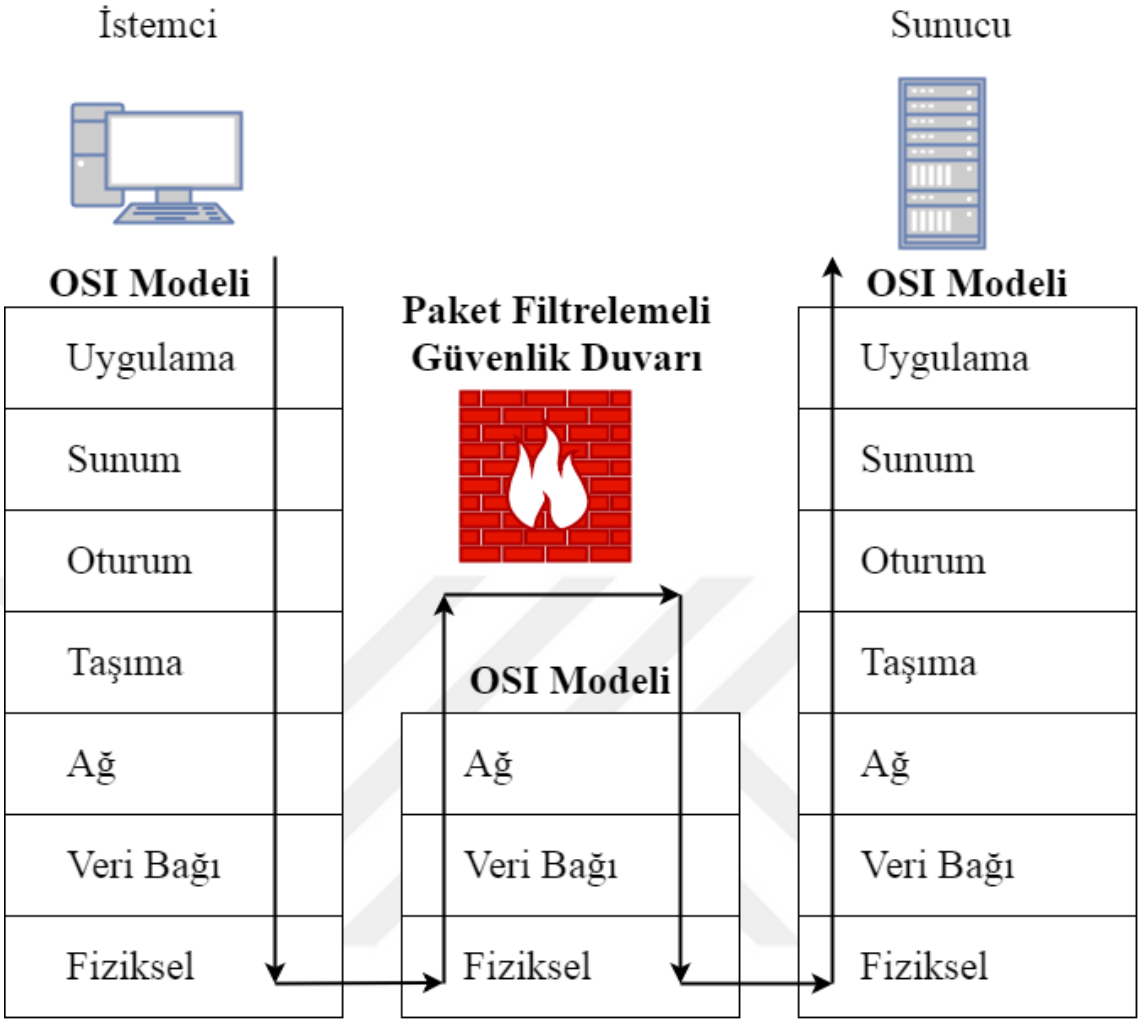
olmaktadır. Belirlenmiş bir mantık çerçevesinde oluşturulan güvenlik politikası ile ağ üzerindeki veri akışına hâkim olunmalıdır. Günümüzde bütün kurumlar özel iç ağları ile genel ağ adını verdiğimiz internet arasına bir güvenlik duvarı yerleştirmektedir. Güvenlik duvarı iç ağ hakkındaki bilgileri dış dünyadan korumaya da yardımcı olur. Kurumunuza bir güvenlik duvarı kurmak istediğinizde, önümüze çıkan en büyük sorunlardan biri, tek tip bir kurulum yapısının var olmamasıdır. Kurumlardaki ağ yöneticileri hangi güvenlik duvarı yapısının kendilerine daha yararlı olduğunu anlamak için güvenlik duvarları konusunda araştırmalar yapmalıdır (Vacca & Ellis, 2005).

Kavramsal olarak güvenlik duvarları 3 türde incelenebilir. Paket Filtrelemeli Güvenlik Duvarı (Packet Filtering Firewall), Uygulama Katmanı Güvenlik Duvarı(Application Level Gateway), Durum Denetimli Güvenlik Duvarı (Stateful Inspection Firewall) (Fulp, 2013).

3.4.1. Paket Filtrelemeli Güvenlik Duvarı

OSI modelinin ağ düzeyinde veya TCP / IP'nin IP katmanında çalışır. Genellikle bir yönlendiricinin parçasıdırlar. Yönlendirici, paketleri bir ağdan alan ve bunları başka bir ağa yönlendiren bir cihazdır. Paket filtrelemeli Güvenlik Duvarında, her paket iletilmeden önce bir dizi kural ile karşılaştırılır. Pakete ve kurallara bağlı olarak, güvenlik duvarı paketi bırakabilir veya reddedebilir. Bu tür güvenlik duvarlarında paket, 3. katmana kadar fark edilmeden gelebilir. Bu tür güvenlik duvarları inceleme yaparken iletilen paketin bir ağ akışının parçası olup olmadığına bakmaz. Kurallar alıcı ve gönderici uç cihazların 3. katman adresleri, port numaraları ve iletişim protokolü gibi bilgilerden oluşturulabilir. Paket filtreleme güvenlik duvarlarının avantajı, düşük maliyet ve ağ performansı üzerindeki düşük etkileridir (Vacca & Ellis, 2005).

Paket filtrelemeli güvenlik duvarı kuralları yapılandırılırken bir paket her zaman ilk uyan kuraldaki sonuca göre hareket edeceği düşünülerek iki farklı yaklaşım ile oluşturulabilir. “Varsayılan olarak izin ver" veya "varsayılan olarak reddet". "Varsayılan olarak izin ver", özellikle reddedilen trafik dışındaki tüm trafiğin güvenlik duvarından geçmesine izin verir. "Varsayılan olarak reddet", izin verilen trafikler dışında tüm trafiğin güvenlik duvarından geçmesini engeller. Şekil 3.9’da paket filtrelemeli güvenlik duvarının yapısı gösterilmektedir.

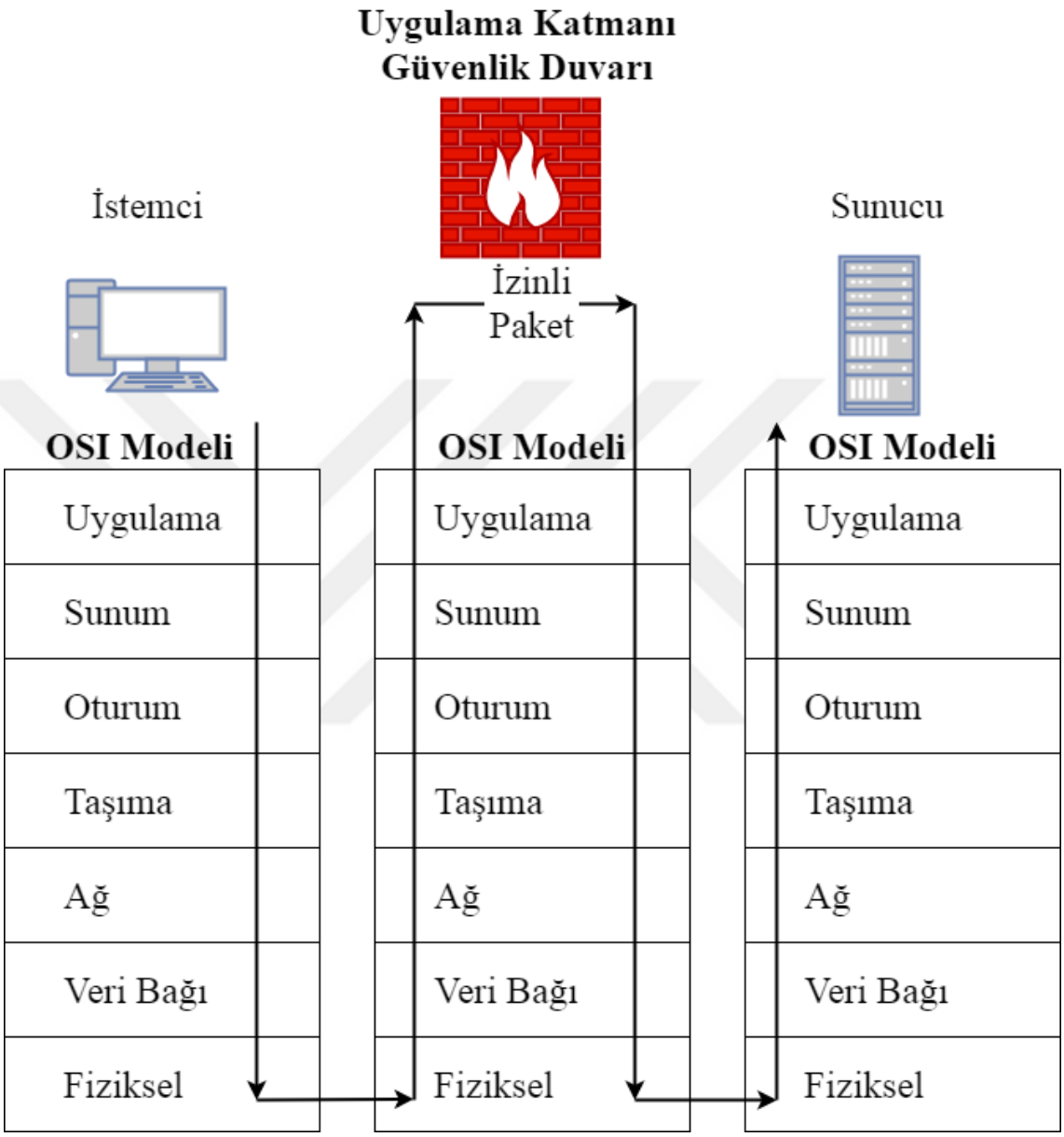


Şekil 3.9. Paket filtrelemeli güvenlik duvarı yapısı

3.4.2. Uygulama Katmanı Güvenlik Duvarı

Bu tür güvenlik duvarları uygulama katmanı da denilen 7. Katmanda çalışır. Bu katmana kadar istenmeyen/tehlikeli trafik ulaşabilir. Uygulama katmanı güvenlik duvarı kendine ulaşan paketin veri kısmına kadar olan tüm başlıkları açabilir/inceleyebilir. Bu tür güvenlik duvarları bir ağ trafiğindeki paketin başlık bilgilerini incelemenin yanında verinin içeriğini de kontrol edebilme yeteneğine sahiptir. Günümüzde çoğu uygulama katmanı güvenlik duvarları aynı zamanda vekil sunucu desteği de sunmaktadır. Bu uygulama şeklinden güvenlik duvarı kaynak ve hedef arasında iletişimi sağlayan bir vekil görevi görmektedir. Bu durumda her iki yönde de iletişim içeriğini kontrol edebilmektedir. İletişimin iki noktasını da birbirlerinden yalıtarak güvenliği olabildiğince

arttırmaktadır (Shinder vd., 2003). Şekil 3.10'da bir uygulama katmanı güvenlik duvarının yapısı gösterilmektedir.

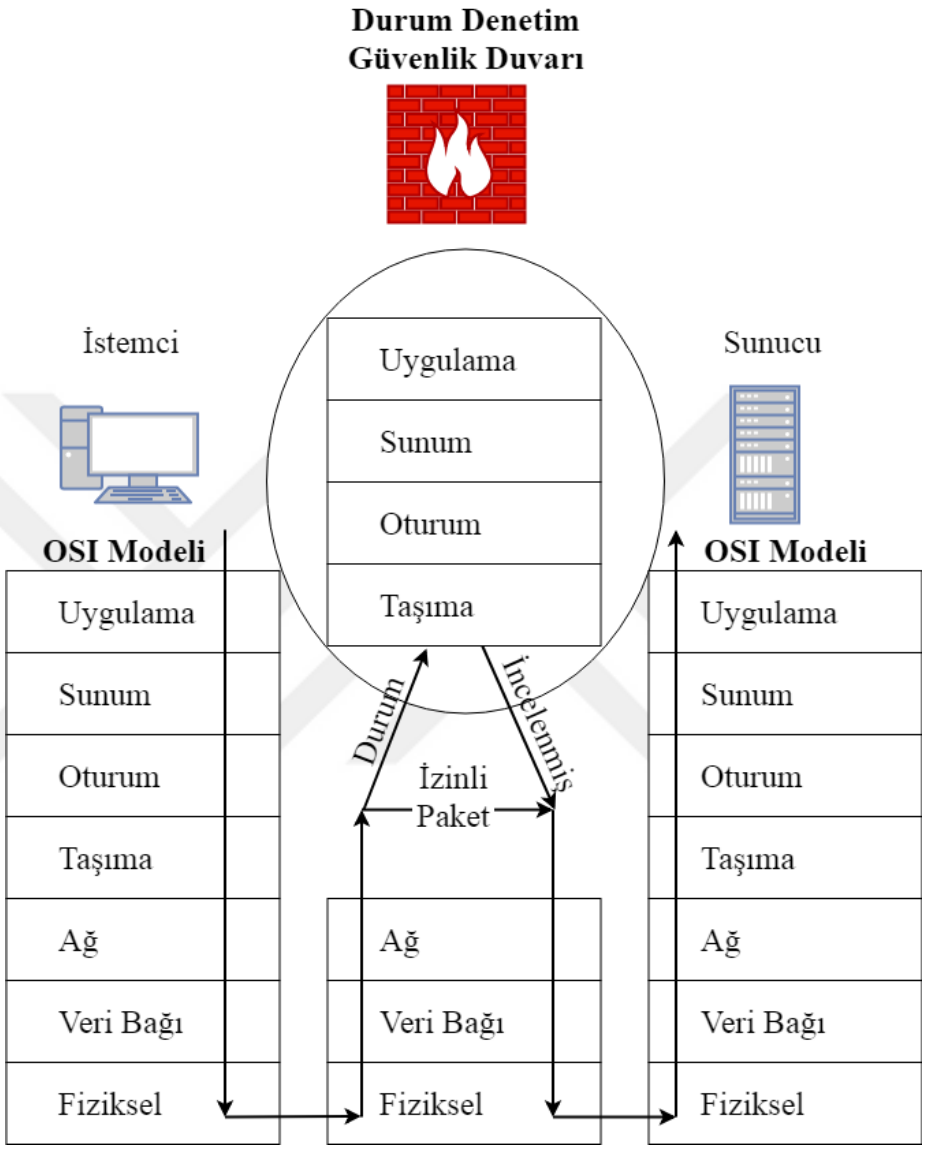


Şekil 3.10. Uygulama katmanı güvenlik duvarı yapısı

3.4.3. Durum Denetimli Güvenlik Duvarı

Durum denetimli güvenlik duvarları paket filtrelemeli güvenlik duvarlarına benzerler; fakat ağa gelen her trafik akşını kaydederler. TCP'de iletişimi ilk başlatan senkronizasyon (SYN) paketi geldiğinde güvenlik duvarı bir durum kaydı oluşturur Bilgisayar ağına yeni paket ulaştığında paketin devam eden bir ağ akışının parçası veya

gereksiz bir paket olup olmadığına karar verebilirler. Bu işlemi yaparken gelen ACK paketinin doğruluğunu tutulan durum tablosu ile karşılaştırırlar. (Goralski, 2017a). Şekil 3.11'de durum denetim güvenlik duvarı yapısı gösterilmektedir.



Şekil 3.11. Durum denetimli güvenlik duvarı yapısı

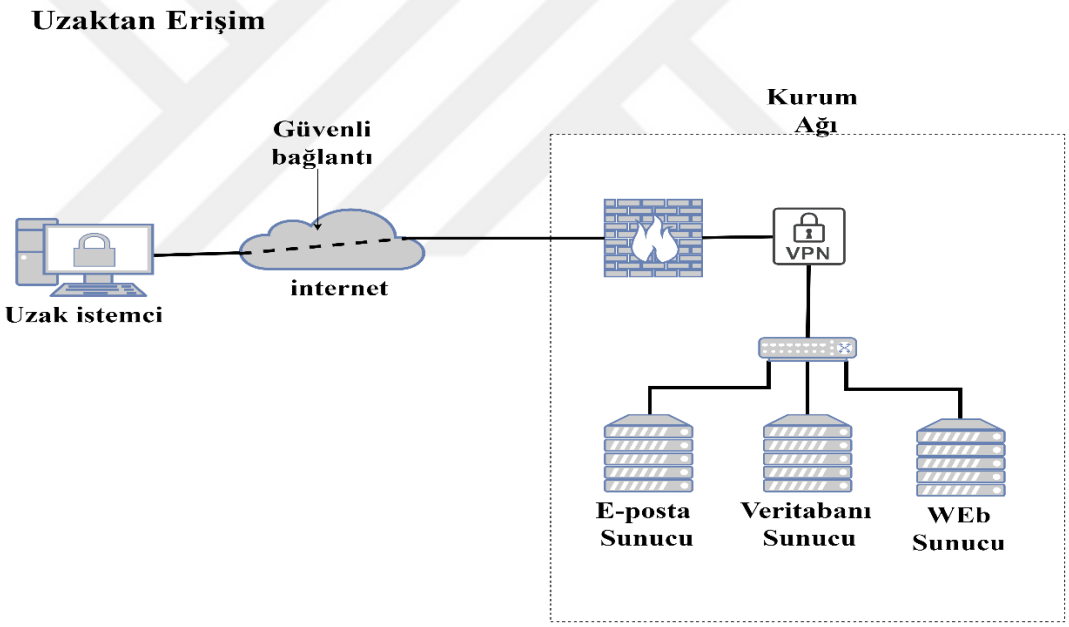
3.5. Sanal Özel Ağlar

Sanal özel ağlar (VPN) ağ yöneticileri için güvenli olmayan bir ağ yapısı ile iki uç düğümü birbirine güvenlik protokolleri ile bağlayan bir güvenlik çözümüdür. Her kurumsal ağ yapısında bulunan sunucular, web sayfaları ve veri tabanları gibi o kurumun temel ağ kaynaklarını oluşturan yapılar mevcuttur. Kaynakları uzakta olan kullanıcıların o yerel alan ağının İçindeymiş gibi güvenle kullanma isteği VPN gibi çözümlerle sağlanır.

VPN sadece uzak kullanıcıları değil kurumlara ait farklı noktalardaki şubeleri de birbirine güvenle bağlamak için çözümler sunar. Bu istekleri gerçekleştirirken VPN, kiralanan maliyetli özel bağlantılar yerine internet gibi genel bir ağı kullandığı için kurumlar tarafından tercih edilmektedir (Stallings, 2011).

3.5.1. Uzaktan Erişim Sanal Özel Ağ

Uzaktan erişim sanal özel ağlar kurum dışından kurum İçindeki kaynaklara internet gibi genel bir ağ yardımıyla bağlanmalarını sağlar. Uzak bağlantıyı yapan kişiler kaynaklara erişim yetkisi alabilmek için; kullanıcı adı ve şifre sorgulamasından geçer. Bu bağlantı, özel bir ağ üzerinden oluyormuş gibi işlem görür. Kuruma bağlanılan genel ağın ne olduğu önemli değildir (Shinder, 2007). Şekil 3.12'de Uzak erişim sanal özel ağın yapısı gösterilmektedir.

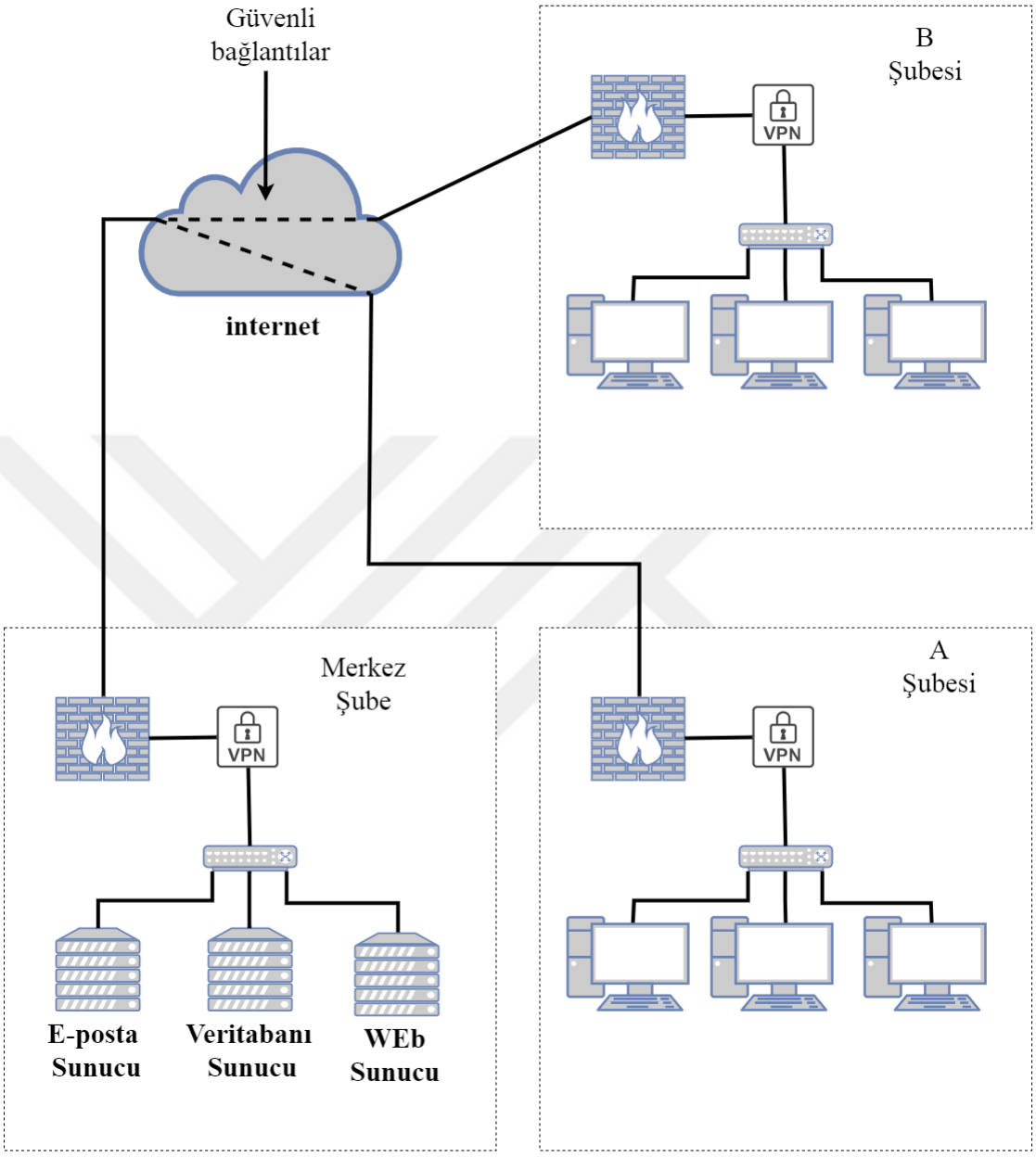


Şekil 3.12. Uzak erişim sanal özel ağ

3.5.2. Siteden Siteye Sanal Özel Ağlar

Birden fazla bölgede birbirinden uzak şubeleri bulunan kurumların, şubelerini birbirine veya merkeze internet gibi bir genel ağ ile bağlama yöntemidir. Bu çözümde aralarında sanal özel ağ kurulan noktalarda bulunan cihazlar karşılıklı olarak yapılandırılmalıdır (Davie & Farrel, 2008). Şekil 3.13'te siteden siteye sanal özel ağ yapısı görülmektedir.

Siteden siteye

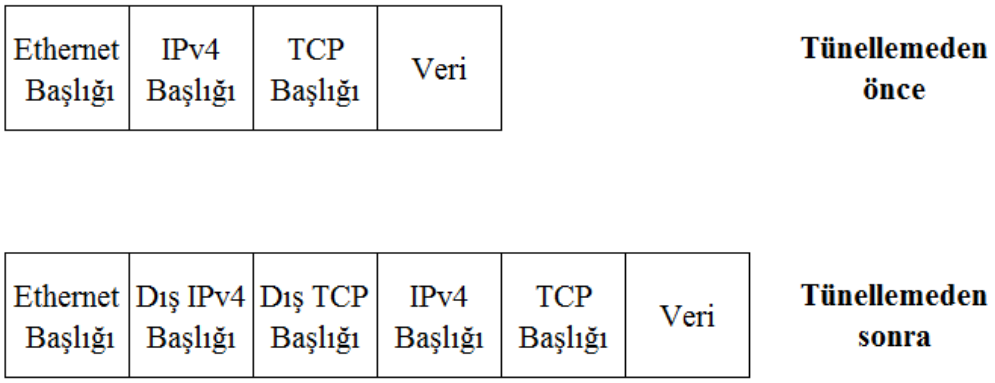


Şekil 3.13. Siteden siteye sanal özel ağ yapısı

3.5.3. Sanal Özel Ağ Tünelleme Protokolleri

VPN internet gibi genel bir ağ üzerinden, bu erişimi güvenli hale getirebilmek için tünelleme adı verilen bir yöntemi kullanır. Bu yöntem bir veri paketini bir başka veri paketinin içine yerleştirerek gerçekleştirir. Bu işlemler tünelleme protokolleri adı verilen protokoller aracılığı ile yapılır. Bu tünelleme protokolleri IPSec, PPTP, L2TP ve SSL/TLS'tir (Alpern & Shimonski, 2010).

Tünelleme işlemi TCP/IP paket yapısını yeni bir paket içine alır. Tünelleme basit bir anlatımla Şekil 3.14'te gösterildiği gibidir (Yüksel & Örencik).



Şekil 3.14. Tünelleme

3.5.3.1. IPSec

Bu tünelleme protokolü için gereken şifreleme ve şifre çözme maliyeti oldukça fazladır. OSI katman üç'te çalışan bu protokol, hala birçok üretici tarafından kullanılmaktadır. Bu prtotokolün, tampon bellek taşmalarına karşı zafiyetleri mevcuttur (Harmening, 2017).

3.5.3.2 PPTP

1999 yılında Microsoft, Ascend, 3COM ve diğer birkaç şirket tarafından oluşturulmuştur. Bu anlamda Microsoft bilgisayarlarda çok yaygındır. IPSec kadar güvenilir değildir fakat işlem maliyeti daha azdır. Windows sunucularında sıklıkla kullanılır (Harmening, 2017).

3.5.3.3. L2TP

OSI modelinin beşinci katmanı olan oturum katmanında çalışır. PPTP den daha güvenli olsa da daha hantal ve her iki bağlanan düğümü de kimlik doğrulama

denetiminden geçmeye zorlar. Çoğu üretici IPSec ve L2TP'yi beraber kullanır (Harmening, 2017).

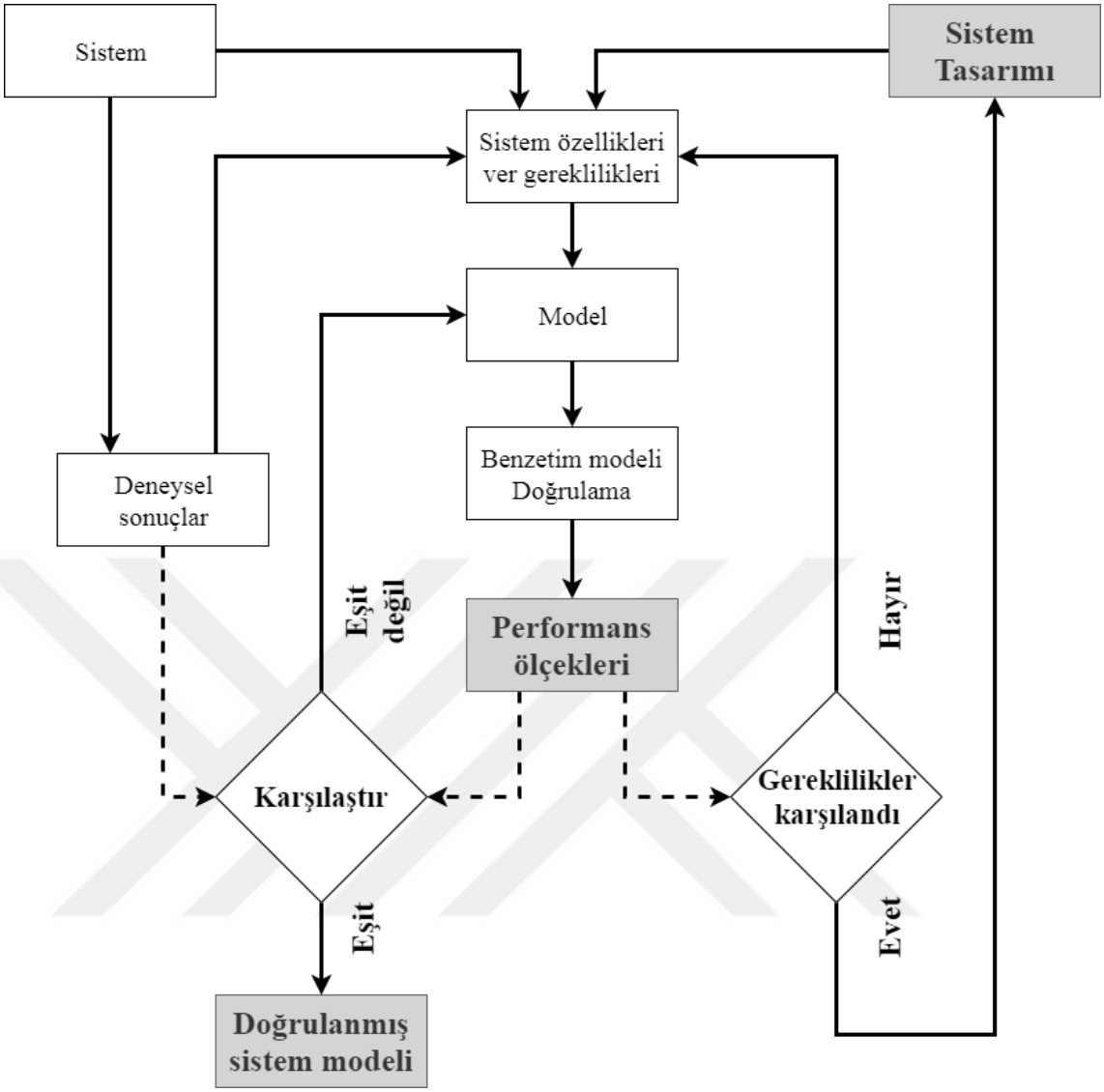
3.5.3.4. SSL/TSL

Bilgisayarların verileri ağ üzerinden gönderilirken dinlenmesini engeller. SSL ve TLS aynı şekilde çalışır. İki bilgisayar haberleşirken önce hangi şifreleme yöntemini kullanacaklarını belirlerler ve ardından birbirleri ile anahtar paylaşımı yaparlar. Bu işlemin ardından iletişim başlar ve bazen bağlantının uçları arasında sertifika konusunda uyuşmazlıklar çıkar bu da iletişimin kesilmesine sebep olur (Harmening, 2017).

BÖLÜM 4

AĞ MODELLEME/BENZETİM VE OPNET

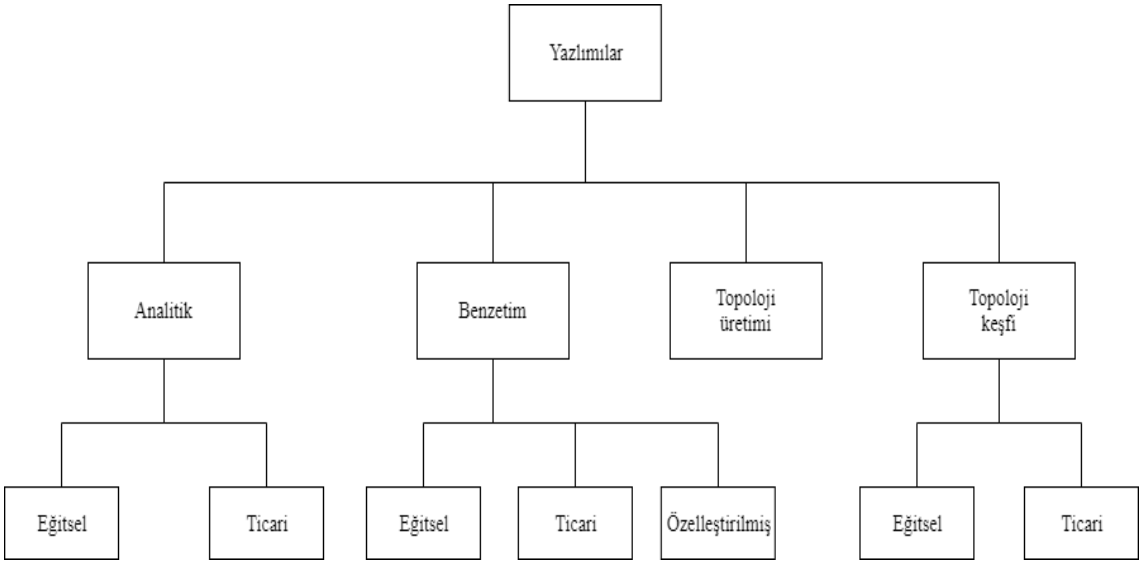
Bilgisayar ağları çok uzun zamandır insanların günlük işlerinin bir parçası konumundadır. Alışveriş, eğlence, eğitim vb. birçok işlemlerin gerçekleştirildiği sistemlerin alt yapısı konumundadır. Bu isteklerin her geçen gün artması ve bu artışa ağ alt yapılarının cevap verebilmesi için sürekli yeni teknolojiler, uygulamalar ve fikirler ortaya çıkmaktadır. Yeniliklere ayak uydurabilmek için bir ağın belli aralıklarla performansının takip edilmesi ve artan isteklere cevap verip veremeyeceği sorusu cevaplanmalıdır. Bu işlemi gerçek ağ üzerinde yerine getirmek zaman ve maliyet açısından çok iyi sonuçlar doğurmayabilir. Diğer bir yandan, sürekli kullanılan bir sistemi güncellemek istediğinizde oluşabilecek aksaklıkların ağ altyapısını sekteye uğratabileceği gerçeği de mevcuttur. Bir ağda yapacağımız değişiklikler hakkında farklı yollardan tespitler yapmak işimize yarayacaktır. Sadece var olan bir ağın değil yeni kurulacak bir ağ alt yapısının da istekleri karşılayıp karşılamayacağını belirlemek iyi olacaktır. Bu ve benzeri sorunların üstesinden gelip ağ yapımızın farklı senaryolarda ne yapacağını tespit etmek için ağ modelleme ve benzetim araçlarını kullanırız. Modelleme, oluşturulmak istenilen yapının mantıksal temsili; benzetim ise oluşturulan mantıksal yapının gerçek dünyadaki davranışını önceden belirlenmiş kurallar bütünü ile denenmesi denilebilir. Şekil 4.1'de bir modelleme ve benzetim çalışmasının akış şeması gösterilmektedir (Suárez, Nuño, Granda, & García, 2015).



Şekil 4.1. Modelleme ve benzetim akış şeması

4.1. Benzetim ve Modelleme Araçları

Benzetim ve modelleme araçları Şekil 4.2'de görüldüğü gibi sınıflandırılabilir (Rahman, Pakštas, & Wang, 2009).



Şekil 4.2. Benzetim ve modelleme araçları sınıflandırılması

Bilgisayar ağlarının modellenmesi ve benzetimi için kullanılan birçok yazılım mevcuttur. Bunların en bilinenleri şunlardır (Gürtürk & Daş, 2017) :

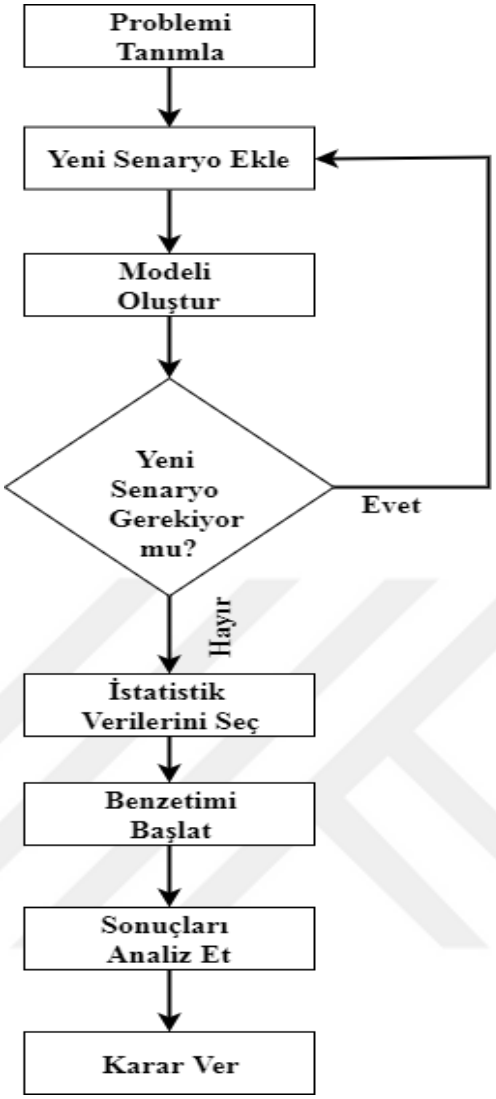
- **OPNET Modeler:** MIT'de ağ dersi eğitiminde kullanılması için Alain Cohen, Marc Cohen ve Steven Baraniuk ortaklığında geliştirilmiştir. Temel amaç bilgisayar ağlarının optimizasyonunu sağlamak için bir benzetim ortamı sağlamaktır. Ticari ve eğitim sürümleri mevcuttur. Windows'ta ve Unix tabanlı sistemlerin birçoğu üzerinde çalışır.
- **OMNeT++:** C++ ile geliştirilmiştir. Benzetim kütüphaneleri C++ ile yazılır. Sadece bir ağ benzetim programı değildir; aynı zamanda başka benzetim yazılımlıları da geliştirmeyi destekleyecek bir çerçevedir.
- **Network Simulator 2:** C++ dili ile yazılmıştır. Genel kamu lisansı ile dağıtılmaktadır. Benzetim nesnelere oTcl diliyle yazılır.
- **Boson NetSim**: Asıl olarak bir yönlendirici benzetim aracıdır. Birçok yönlendirme protokolü ile LAN/WAN protokollerini de destekler. Cisco cihazları için benzetim ortamı sağlar.
- **Cisco Packet Tracer:** Ağ eğitimi için Cisco firmasının geliştirdiği bir üründür. Topolojiler modellemeyi, ağ İçinde akan trafiği takip etmeyi, ağdaki belli bir andaki paketleri incelemeyi ve ağ cihazları yapılandırmayı da içeren bir dizi imkân sunar (Makasiranondh, Maj, & Veal, 2010). Son sürümlerinde IoT benzetim desteği de sunmaktadır.

- **GNS3:** Cisco Packet Tracer'ın alternatifi sayılır. Uzmanlık sertifikaları almak ve eğitim içeriğini yükseltmek için iyi imkânlar sunar. Sanallaştırma yazılımları ile beraber kullanılabildiği için çok iyi bir benzetim ortamı sunar (Makasiranondh vd., 2010).

4.2. OPNET Modeler

OPNET Modeler, iletişim ağlarının modellenmesi ve benzetimi için çok geniş ek kütüphaneler ile birlikte grafik arayüz destekli kapsamlı bir içerik sunar. Bir LAN yapısından, WAN yapılarını ve hatta uydu ağlarına kadar birçok ağ yapısının modellenmesine ve benzetimine imkân sağlar. OPNET ile ilgili temel özellikleri aşağıdaki gibi sıralayabiliriz (Chang, 1999):

- **Model ve benzetim döngüsü**: OPNET Şekil 4.3'te belirtildiği gibi bir çalışma döngüsü kullanır.
- **Hiyerarşik modelleme:** Modelin farklı senaryolardaki davranışları için hiyerarşik bir modelleme ve benzetim yöntemi sunar.
- **İletişim ağlarında uzmanlaşmış:** Ayrıntılı kütüphane yapısı çok farklı protokolleri desteklemekle beraber kişilerin kendi yapılarını oluşturmalarına da olanak sağlar
- **Otomatik benzetim:** Ayrık olay benzetimlerini çok kolay kullanıma sunan ve sonuçları karşılaştırmaya olanak sağlar.



Şekil 4.3. OPNET modelleme ve benzetim döngüsü

4.2.1. OPNET Modeler Düzenleyicileri

OPNET Modeler; proje düzenleyici, düğüm düzenleyici, süreç düzenleyici, bağlantı düzenleyici, paket biçim düzenleyici, ICI düzenleyici, PDF düzenleyici, inceleme düzenleyici vb. bir çok grafik arayüz destekli düzenleyici ile modelleme ve benzetim işlemini kolaylaştıran bir ortam sunar (Lu & Yang, 2012).

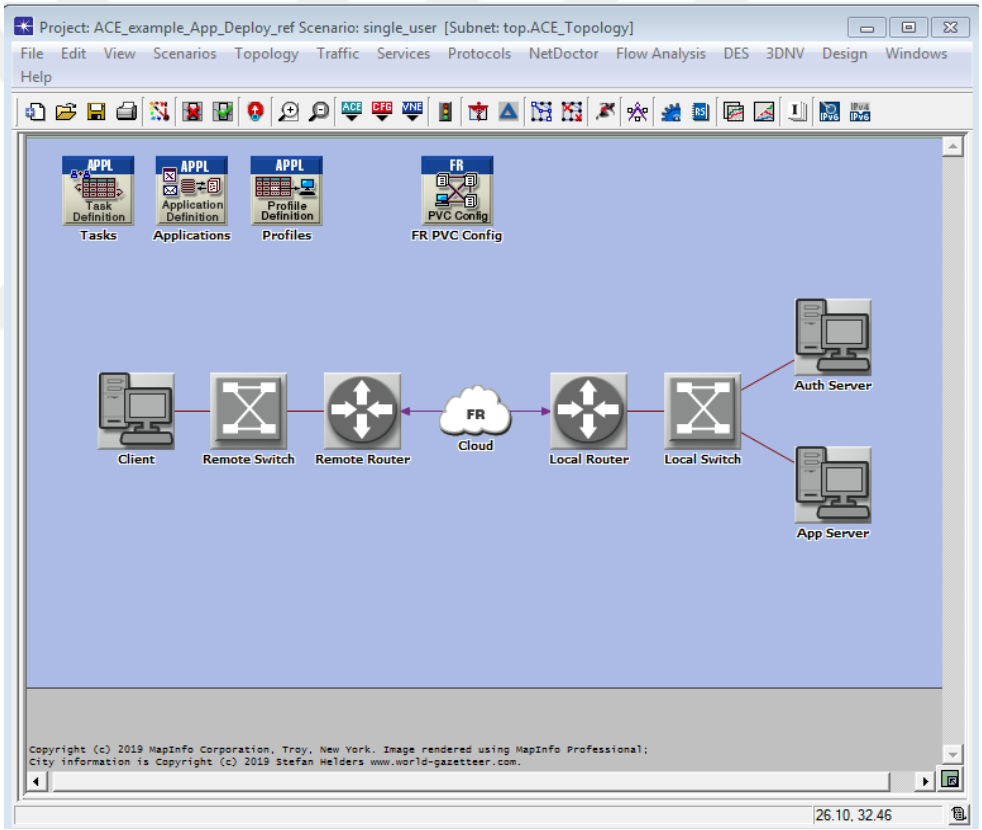
4.2.1.1. Proje Düzenleyici

OPNET Modeler ile oluşturulacak ağ modelleri üç katmandan oluşur: Ağ modeli, düğüm modeli ve işlem modeli. Ağ modeli proje düzenleyicisinde oluşturulur. Ana düzenleyici sayılabilecek bu kısımda, birçok bileşen ve ağ bağlantısı ile çok farklı ağ

yapıları modellenebilir. Bu düzenleyicide yapılabilecek işlemler şöyle sıralanabilir (Lu & Yang, 2012):

- Ağ modelleri oluşturma ve düzenleme
- Projelere ait farklı senaryoları yönetme
- Ağ topolojileri yapılandırma
- Ağ trafiği yapılandırma
- Ağ ortam değişkenlerini özelleştirme
- Hat bağlantı doğrulama
- Farklı alt ağlara ait paket akışını yakalama

Şekil 4.4'te proje düzenleyici ekranı gösterilmektedir.

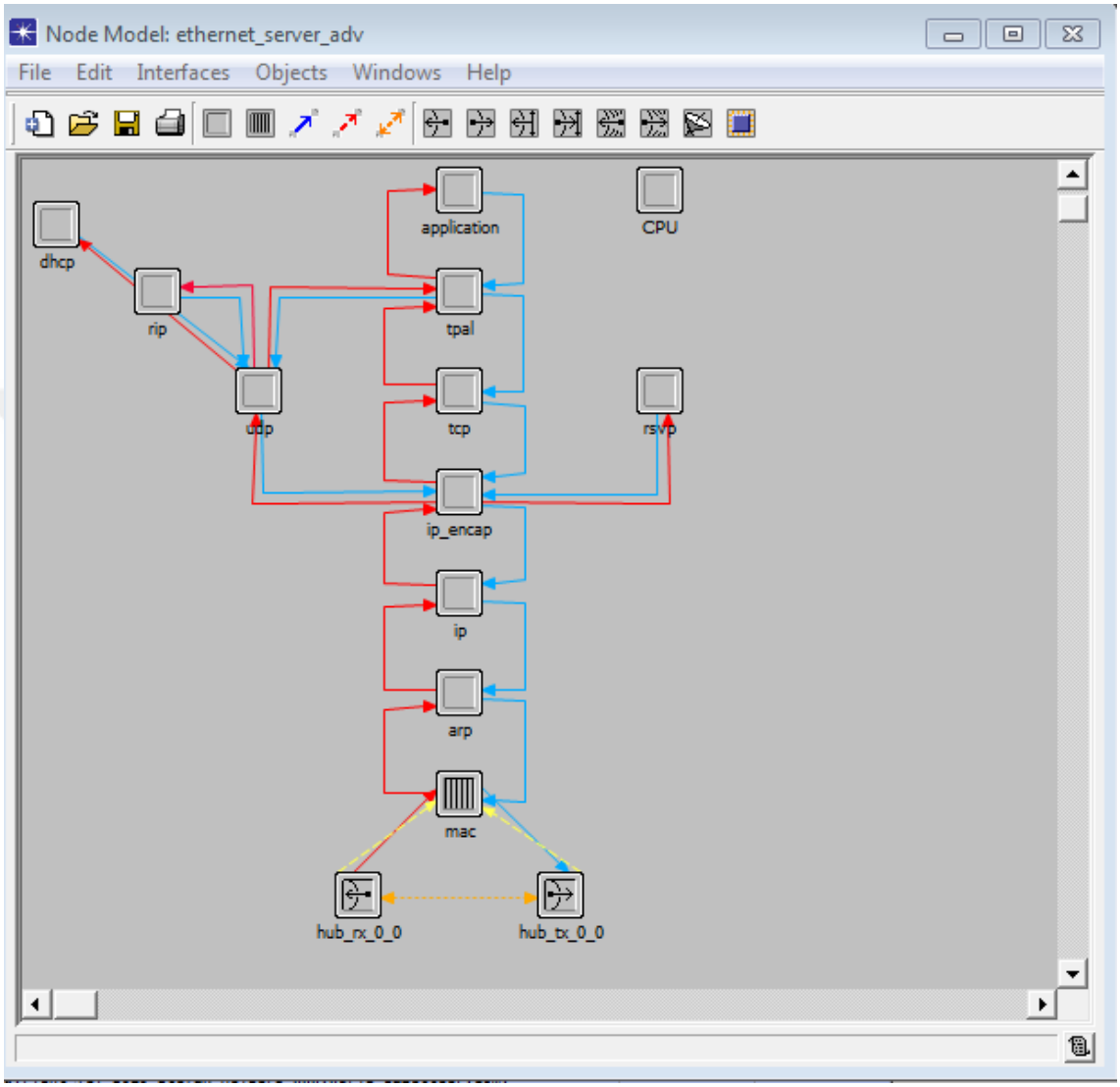


Şekil 4.4. Proje düzenleyici

4.2.1.2. Düğüm Düzenleyici

OPNET'te modele dahil olan yapılar düğüm düzenleyici ile tanımlanmıştır. Var olan düğümleri düzenlemeye veya yeni düğümler eklenmesine olanak sağlar. Her düğüm

ağ yapısında iletişim paketleri ile işlemler yapacak şekilde yapılandırılır (Svensson & Popescu, 2003). Şekil 4.5'te bir Ethernet sunucunun düğüm düzenleyicideki yapısı gösterilmektedir.

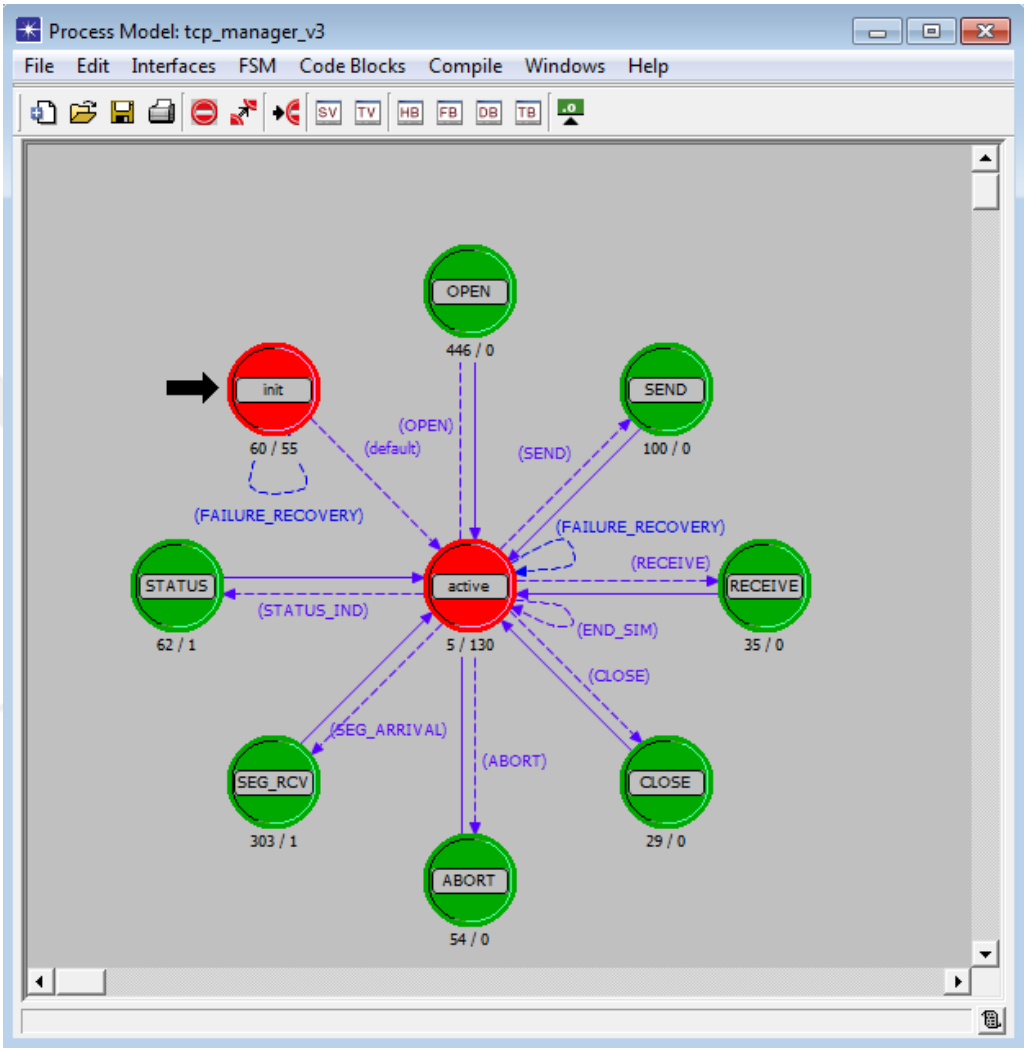


Şekil 4.5. Düğüm düzenleyici

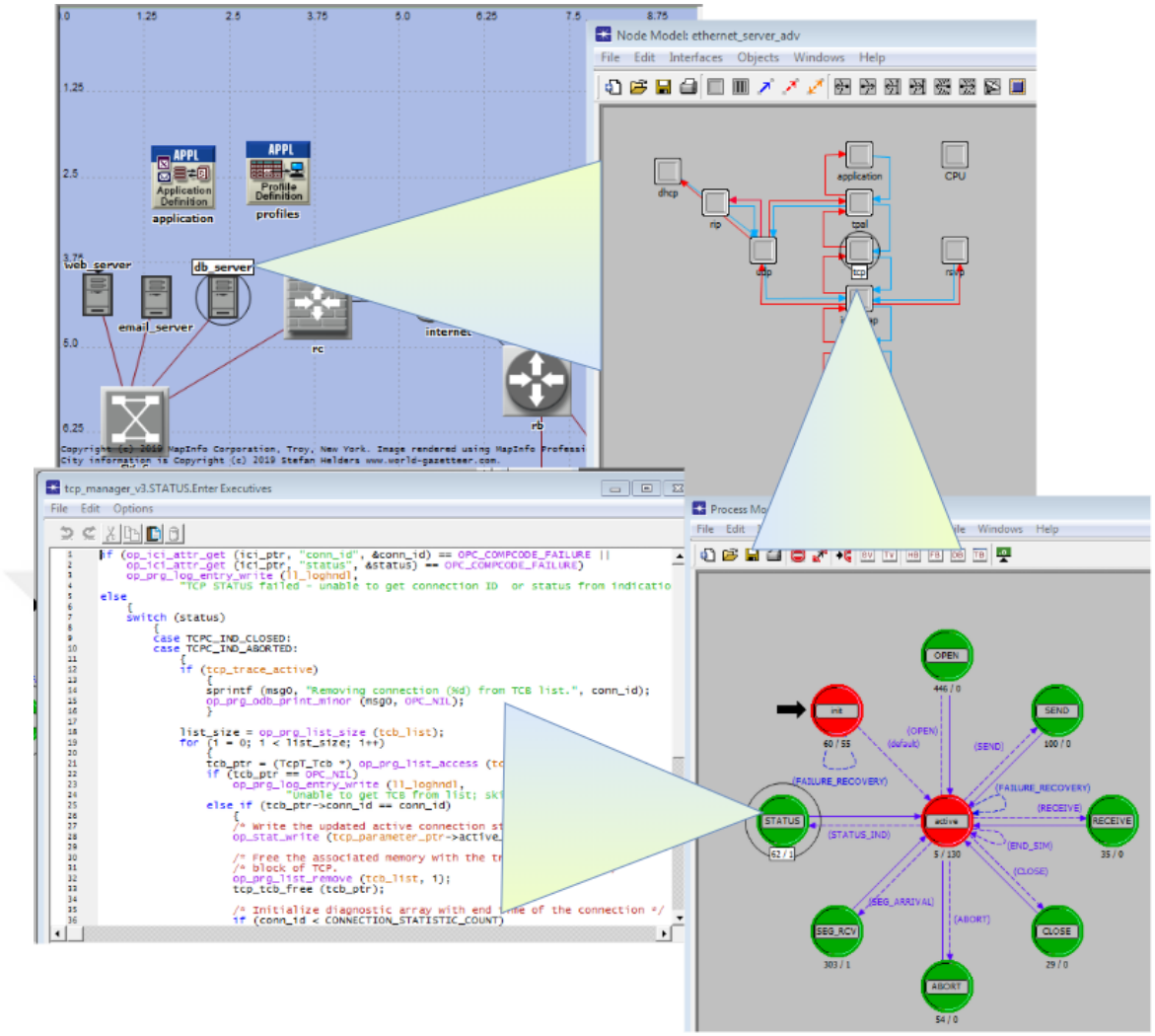
4.2.1.3. Süreç Düzenleyici

Bir süreç modeli, benzetim ortamında çalışan algoritmaların taşıyıcısıdır. Süreç düzenleyici bu yapıların düzenlenmesini sağlar. Bu yöntem ile İletişim protokolü, algoritma, kuyruk stratejisi, paylaşılan kaynak vb. dahil olmak üzere çoğu yazılım veya donanım yapısının benzetimi yapılabilir (Chen, Miao, & Humar, 2019).

Süreç düzenleyicide süreçler, Sonlu durum makinesi (Finite State Machine-FSM) yardımı ile modellenir (Mohorko, Fras, & Klampfer, 2008). Şekil 4.6'da süreç düzenleyici yapısı görülmektedir. Şekil 4.7'de ise OPNET Modeler yazılımının hiyerarşik modelleme yapısı gösterilmektedir.



Şekil 4.6. Süreç düzenleyici



Şekil 4.7. OPNET Modeler hiyerarşik modelleme yapısı

BÖLÜM 5

METODOLOJİ

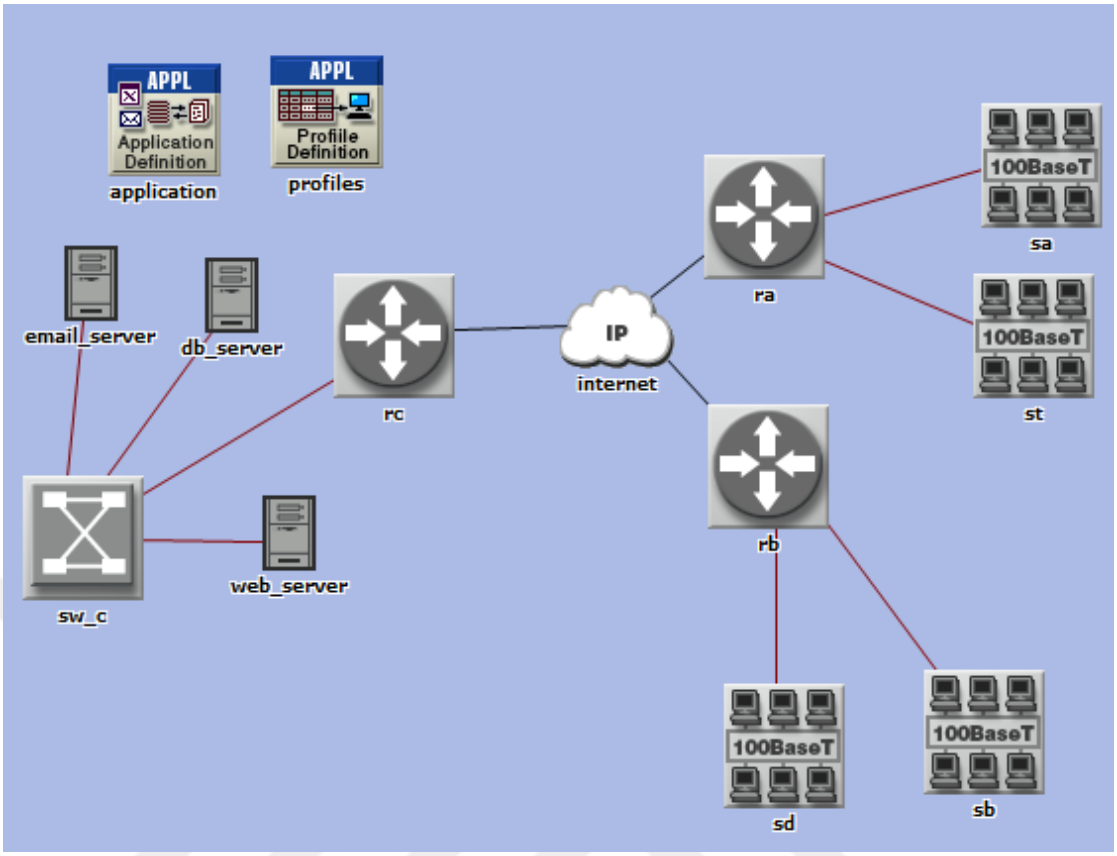
Yapılan çalışmalarda kullanılmış olan ağ modeli günümüzdeki kurumsal ağların yapısı göz önünde bulundurularak oluşturulmuştur. Bunun için üç farklı senaryo üzerinde durularak benzetim sonrasındaki değişiklikler incelenmiştir. Modelleme ve benzetim işlemleri OPNET Modeler yazılımının 14.5 Educational sürümü kullanılarak gerçekleştirilmiştir. Gerçekleştirilen benzetim uygulamalarında 3 ana senaryo yapısında aynı istatistik değerleri senaryolar arasındaki karşılaştırmaların görsel olarak incelenmesi için kaydedilmiştir. Bu amaçla ağ modelimiz, incelenmek istenilen durumların benzetimini gerçekleştirilecek şekilde modellenmiştir.

5.1. OPNET ile Ağın Modellenmesi

Çalışmada bütün senaryo ve ölçümlerin gerçekleştirileceği kurumsal ağı modellemek için OPNET proje editörü kullanılmıştır. Proje editöründe yapılan modellemede amaca uygun olarak üç farklı senaryo oluşturulmuştur:

- "no_firewall_no_vpn": Güvenlik Duvarı ve Sanal Özel Ağın etkin olmadığı senaryo.
- "firewall_no_vpn": Güvenlik Duvarının etkin, Sanal Özel Ağın etkin olmadığı senaryo.
- "firewall_vpn": Güvenlik Duvarı ve Sanal Özel Ağın etkin olduğu senaryo.

Kullanılacak temel topoloji Şekil 5.1'de gösterilmiştir.



Şekil 5.1. Kullanılan Modelin Topolojisi

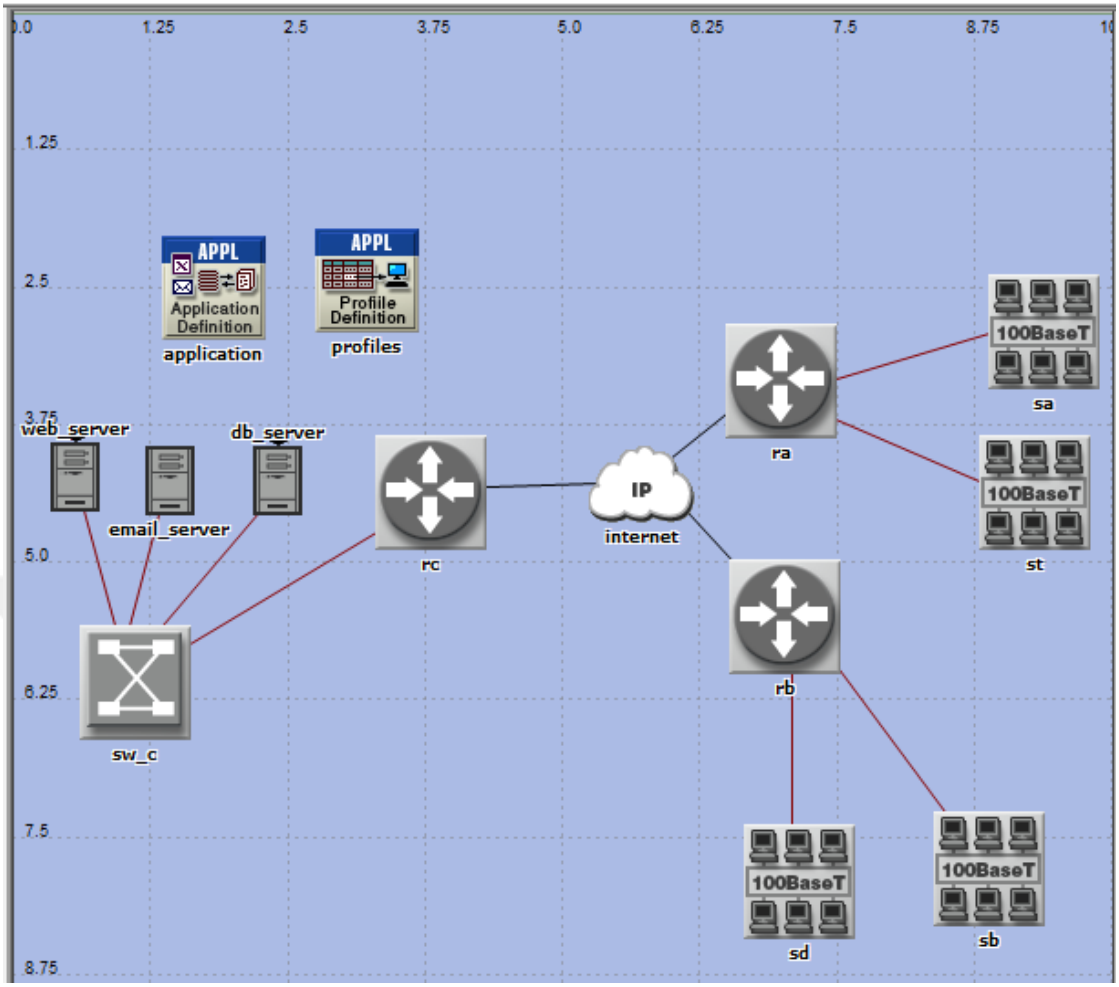
Topolojinin gerçekleştirilmesi için OPNET Modeler projesine Çizelge 5.1'de ifade edilen nesneler dahil edilmiştir.

Çizelge 5.1. Topolojide Kullanılan Nesneler

Sıra No	Nesne Adı	Nesne Modülü	Özellikler	Adet
1	application	Application Config	-	1
2	profiles	Profile Config	-	1
3	vpn	IP VPN Config	IPSec Tünelleme	1
4	sa, sb, sd, st	100BaseT_LAN		4
5	ra, rb, rd	ethernet4_slip8_gtwy	4 Ethernet bağlantısı 8 Seri hat IP bağşantısı	3
6	rc	ethernet4_slip8_gtwy/ ethernet2_slip8_firewall	1 Ethernet bağlantısı 1 Seri hat IP bağşantısı	1
7	internet	ip32_cloud	-	1
8	sw_c	ethernet16_switch	16 Ethernet bağlantısı (10, 100, 1000 Mbps)	1
9	web_server, db_server, email_server	ethernet_server	Dell PowerEdge 1855, 2 CPU, 1 Core(s) Per CPU, 3600MHz, Win2003, System	3
10	-	100BaseT Duple Link	-	8
11	-	PPP_DS1 Duplex Link	-	4

5.2. Ağ Modelinin Ayarlarının Yapılması

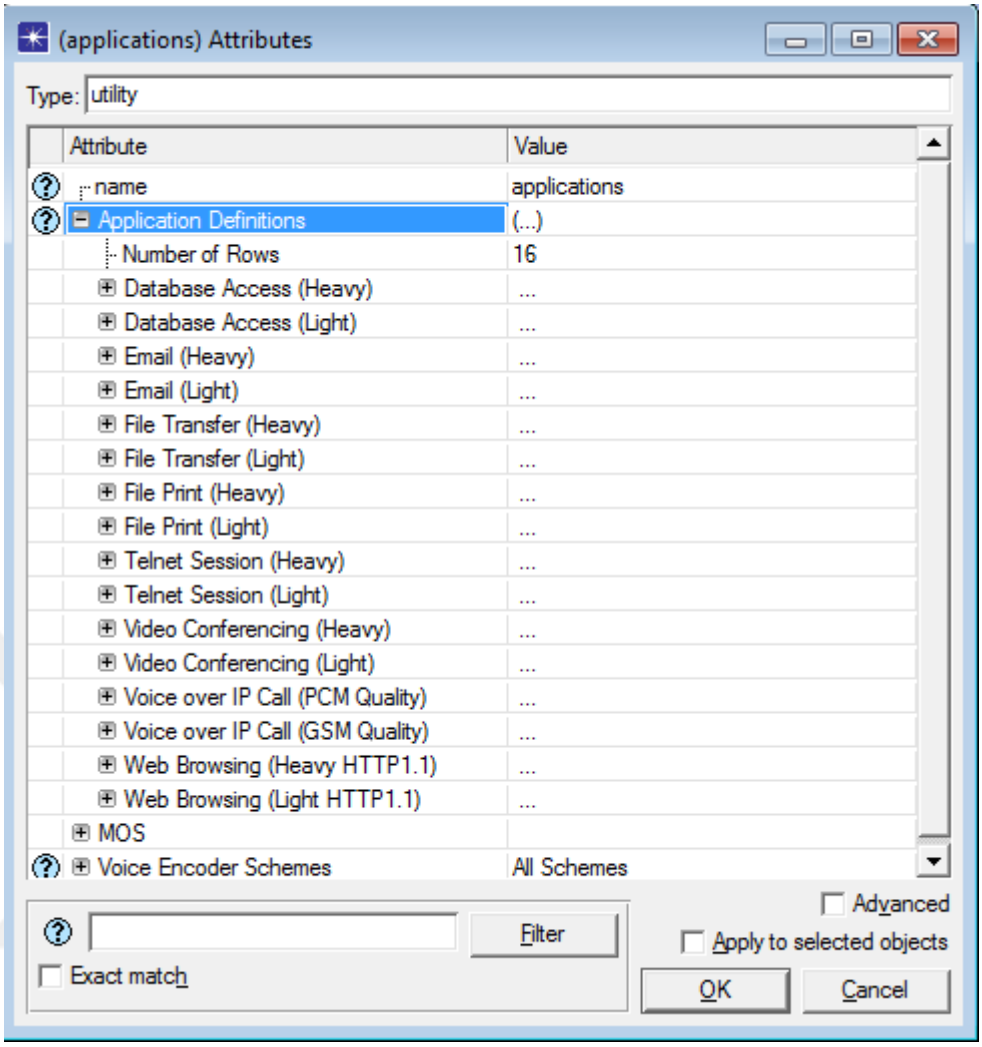
OPNET ile oluşturulan ağ modeli ilk senaryo olan “no_firewall_no_vpn” adı ile kaydedilmiştir. Bu ilk senaryoda yapılan ayarlamalar, diğer 2 senaryoya temel oluşturacak şekilde yapılmıştır. Bu nedenle ilk senaryoda Şekil 5.2’de gösterildiği gibi güvenlik duvarı ve sanal özel ağ uygulamalarına yer verilmemiştir.



Şekil 5.2. "no_firewall_no_vpn" senaryosu

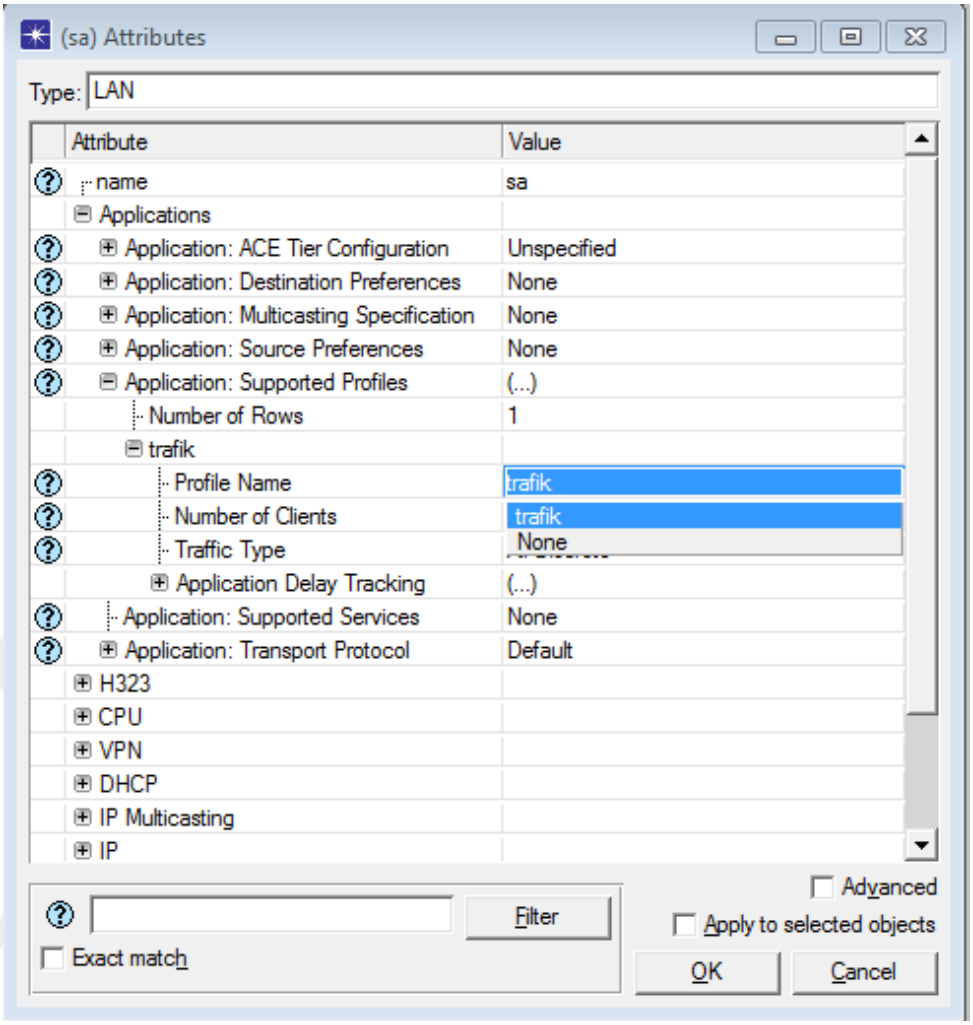
5.2.1. Güvenlik Duvarı ve Sanal Özel Ağ Etkin Olmayan Senaryonun Ayarları

Oluşturulan modelde çalışacak uygulamaların tanımlanması **'Application Config'** nesnesi üzerinden gerçekleştirilmiştir. İstemci ve sunucu bilgisayarlarda etkin olarak çalışması istenilen veri tabanı, e-posta ve web uygulamaları göz önüne alındığında **'Application Definitions'** nitelik kısmından **'Default'** seçeneği seçilerek OPNET Modeler yapısında bulunan hazır ayarlar Şekil 5.3'te gösterildiği gibi etkin hale getirilmiştir.



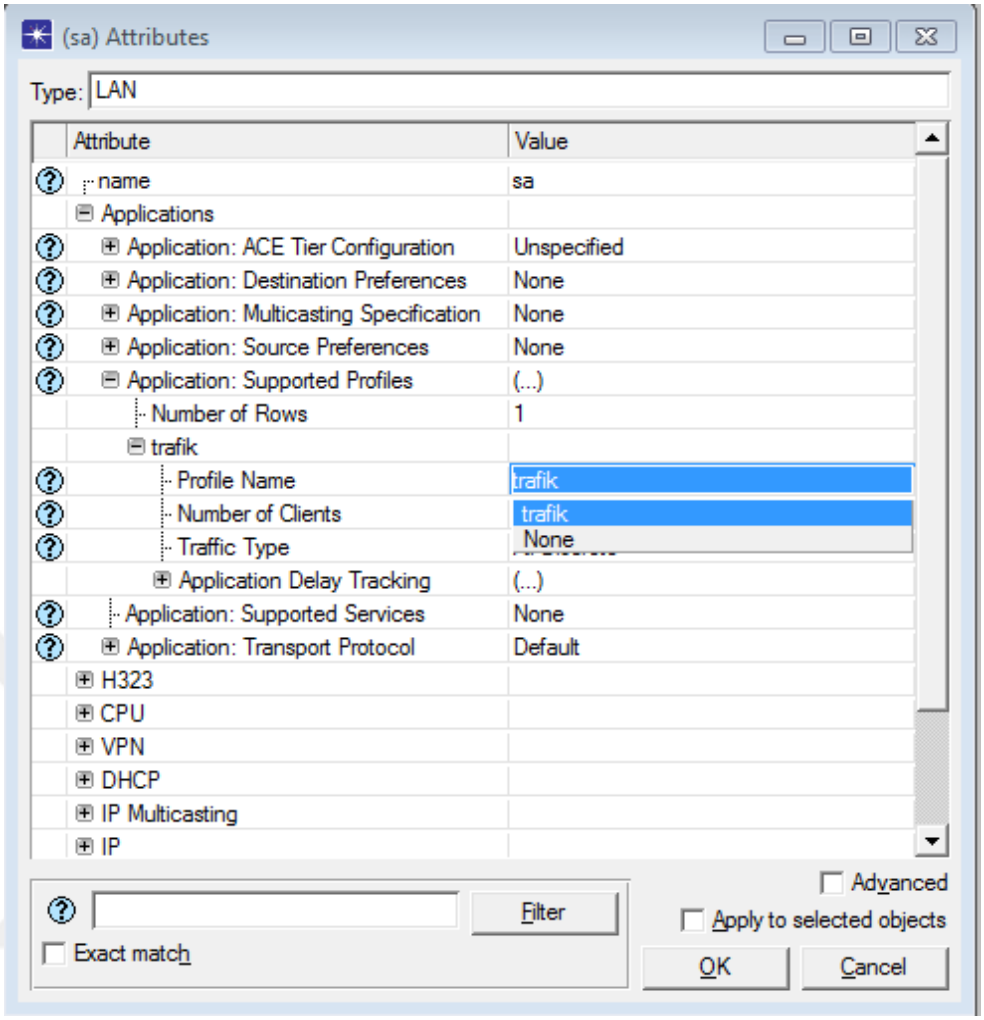
Şekil 5.3. Application Config nesnesi uygulama ayarları

Bu uygulama ayarlarını kullanarak istemci cihazlardan sunucu cihazlara ağ trafiği profilinin ayarlanması için **'Profiles Config'** nesnesi İçinden **'Profile Configuration'** niteliğinin yapılandırılması gerekmektedir. Bu işlem için Şekil 5.4'te gösterildiği biçimde gerekli ayarlamalar yapılarak, istemcilerden veri tabanı, e-posta ve web sunucularına ağ trafiği oluşturacak **'trafik'** adında bir profil oluşturulmuştur.



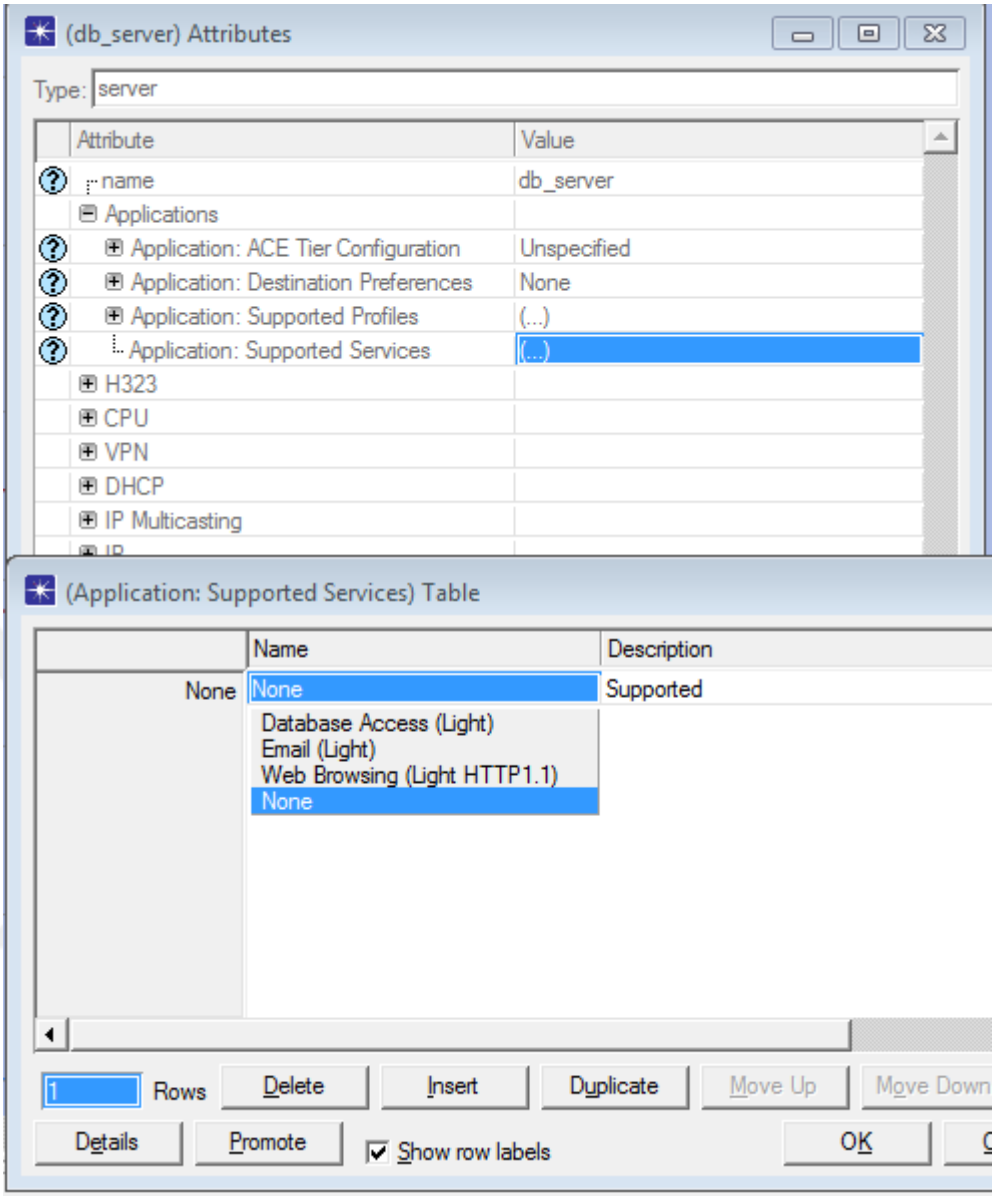
Şekil 5.4. 'Profiles Config' nesnesi profil ayarları

Modelde bulunan **'ra'**, **'rb'** yönlendiricilerine bağlı dört alt ağ ile temsil edilen ve trafiği oluşturacak olan istemci cihazlara, **'Profiles Config'** te oluşturulan **'trafik'** profili Şekil 5.5'te gösterildiği gibi **'Application: Supported Profiles'** niteliğine uygulanarak bu cihazların benzetim anında ağda trafik oluşturmaları sağlanmıştır. Bu ayarların uygulandığı **'sa'**, **'sb'**, **'sc'** ve **'sd'** alt ağlarının her birine 200 adet istemci cihaz tanımlanması yapılarak ağda 800 adet istemci ile istenen yoğunlukta bir ağ trafiği oluşturulması sağlanmıştır.



Şekil 5.5. İstemci nesnesi profil ayarları

Ağ modelinde istemci bilgisayarların kullanacağı uzak ağda bulunan her uygulama farklı sunucularda yapılandırılarak her uygulama için performans verisi toplanması sağlanmıştır. Daha önce **'Application Config'** nesnesinde tanımladığımız uygulamalar, istemci bilgisayarlara profil olarak ayarlanmıştır. Sunucu bilgisayarlarda ise bu uygulamalar Şekil 5.6'da gösterildiği gibi **'Application: Supported Sevices'** niteliğinden sunucuya ait uygulama seçilerek sunucunun vereceği hizmet olarak ayarlanmıştır.



Şekil 5.6. Sunucu nesnesi profil ayarları

5.2.2. Toplanacak İstatistik Verilerinin Seçilmesi

Diğer bütün senaryolarda ortak toplanacak istaistikleri belirlemek için üç farklı istatistik türünden amaçlara uygun olanlar seçilmiştir. Benzetim anında her senaryodan hangi istatistik verilerinin (**'Global Statistic', 'Node Statistic' 'Link Statistic'**), toplanacağı Çizelge 5.2'de gösterildiği gibi seçilmiştir.

Çizelge 5.2. Seçilen İstatistik Verileri

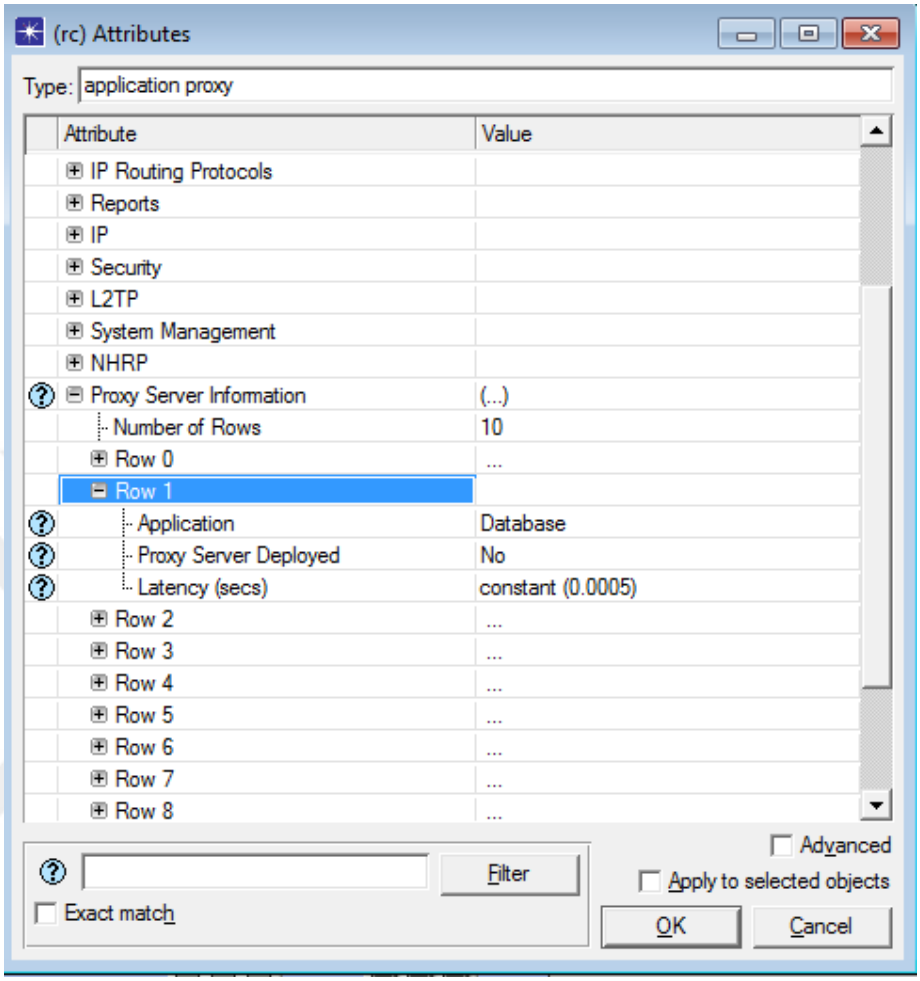
İstatistik Türü	İstatistik Adı	Ölçülen Değer	İstatistik Ölçü Birimi
Global	DB Query	Response Time	saniye
Global	DB Query	Traffic Received	bayt/saniye
Global	Email	Download Response Time	saniye
Global	Email	Traffic Received	bayt/saniye
Global	HTTP	Page Response Time	saniye
Global	HTTP	Traffic Received	bayt/saniye
Link	Point-to-Point-(internet-ra)	Utilization	kullanım
Link	Point-to-Point-(internet-rb)	Utilization	kullanım
Node	Server Performance	Load	istek/saniye

5.2.3. Güvenlik Duvarı Etkin, Sanal Özel Ağ Etkin Olmayan Senaryonun Ayarları

"no_firewall_no_vpn" senaryosunda temel ayarlar yapıldığı için bu senaryodan çoğaltma yapılarak yeni senaryo "firewall_no_vpn" adıyla kaydedilerek ikinci senaryo oluşturulmuştur. **'ethernet4_slip8_gtwy'** model bir yönlendirici olan **'rc'** adlı nesne, senaryoya uygun olarak **'Model'** niteliği **'ethernet2_slip8_firewall'** olarak değiştirilerek güvenlik duvarı olarak yapılandırılması sağlanmıştır.

Güvenlik duvarı haline gelen yeni yönlendirici modelinde uzak ağı temsil eden sunucuların bulunduğu ağdaki veri tabanı uygulamalarına erişimi kısıtlayan şekilde yapılandırılmıştır. Bu işlem için **'rc'** cihazının **'Proxy Server Information'** niteliğinde **'Row1'** satırında bulunan **'Database'** uygulamasının **'Proxy Server Deployed'** değeri Şekil 5.7'de görüldüğü gibi **'No'** olarak değiştirilerek yapılmıştır. Bu yapılan işlemle

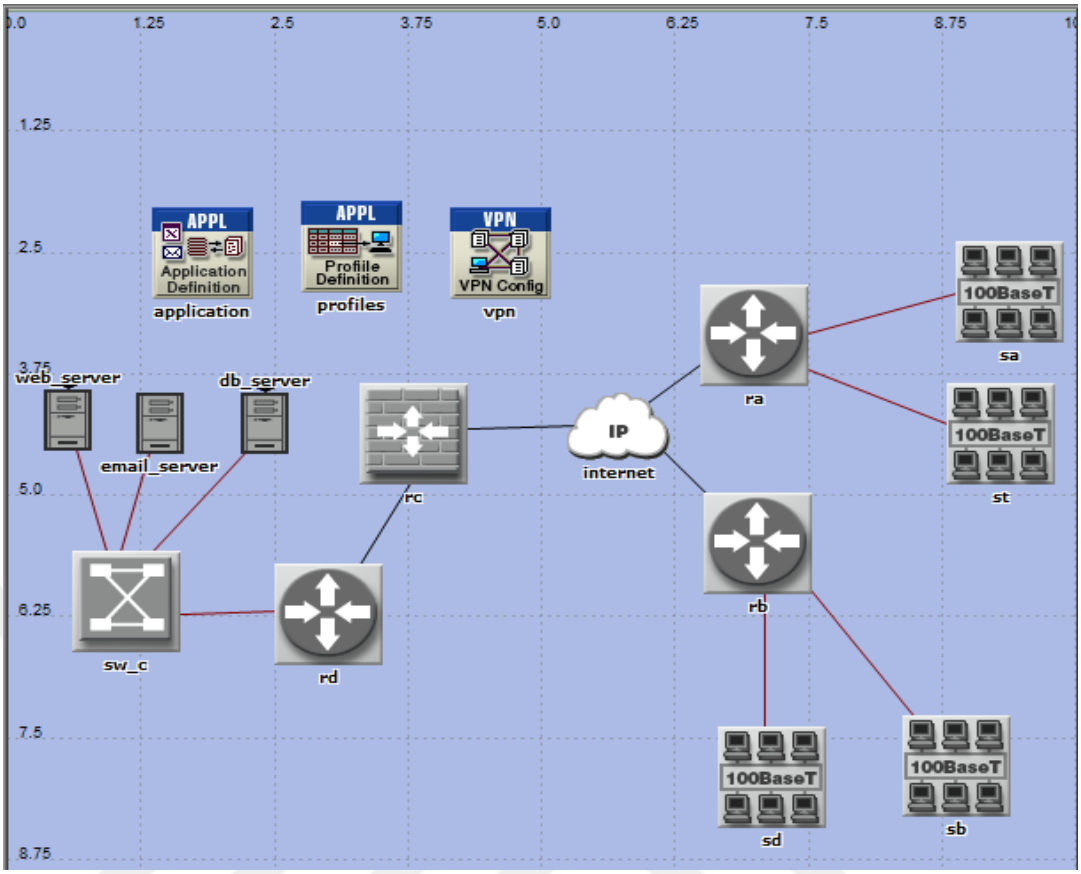
güvenlik duvarı, sunucu bilgisayarların bulunduğu ağdaki veri tabanı isteklerini reddedecek şekilde ayarlanmıştır. Yapılandırılan güvenlik duvarı tipi uygulama



Şekil 5.7. rc nesnesi Güvenlik Duvarı Ayarı

5.2.4. Güvenlik Duvarı ve Sanal Özel Ağ Etkin Olan Senaryonun Ayarları

"firewall_no_vpn" senaryosunda Güvenlik duvarı ayarı yapıldığı için bu senaryodan çoğaltma yapılarak oluşan yeni senaryoya "firewall_vpn" adı verilerek üçüncü senaryo oluşturulmuştur. OPNET Modeler'da proje alanına yeni **'rd'** isimli **'ethernet4_slip8_gtwy'** ve **'VPN'** isimli **'IP VPN Config'** nesnesi eklenerek; **'rd'** isimli yeni yönlendirici sayesinde temsili istemci ağı olan ve **'ra'** yönlendiricisine bağlı **'sa'** alt ağındaki cihazlar ile uzak ağ arasında sanal özel ağ kurulması sağlanmıştır. Bu eklemelerin yapılması ile oluşan yeni modelin topolojisi Şekil 5.8'de gösterildiği gibi oluşturulmuştur.



Şekil 5.8. "firewall_vpn" senaryosu

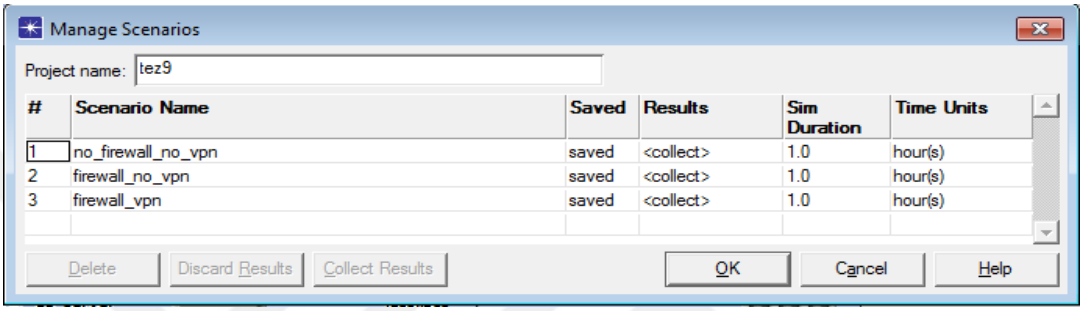
'ra' yönlendiricisine bağlı **'sa'** alt ağı ile 'rd' arasında Sanal Özel Ağ kurulması için eklenen **'IP VPN Config'** nesnesinin '**VPN Confguration'** niteliğine yeni bir satır eklenerek; eklenen yeni satırın **'Tunner Source Name'**, **'Tunnel Destinatin Name'** ve **'Remote Client List'** niteliklerine , Şekil 5.9'da görüldüğü gibi, ra, rd ve sa değerleri girilmiş ve bu sayede sistemde sanal özel ağ etkinleştilmiştir.

Attribute	Value
name	vpn
VPN Configuration	(...)
Number of Rows	1
ra	
Tunnel Source Name	ra
Tunnel Destination Name	rd
Delay Information	None
Operation Mode	Compulsory
Remote Client List	(...)
Number of Rows	1
sa	
Client Node Name	sa

Şekil 5.9. 'IP VPN Config' nesnesi ayarları

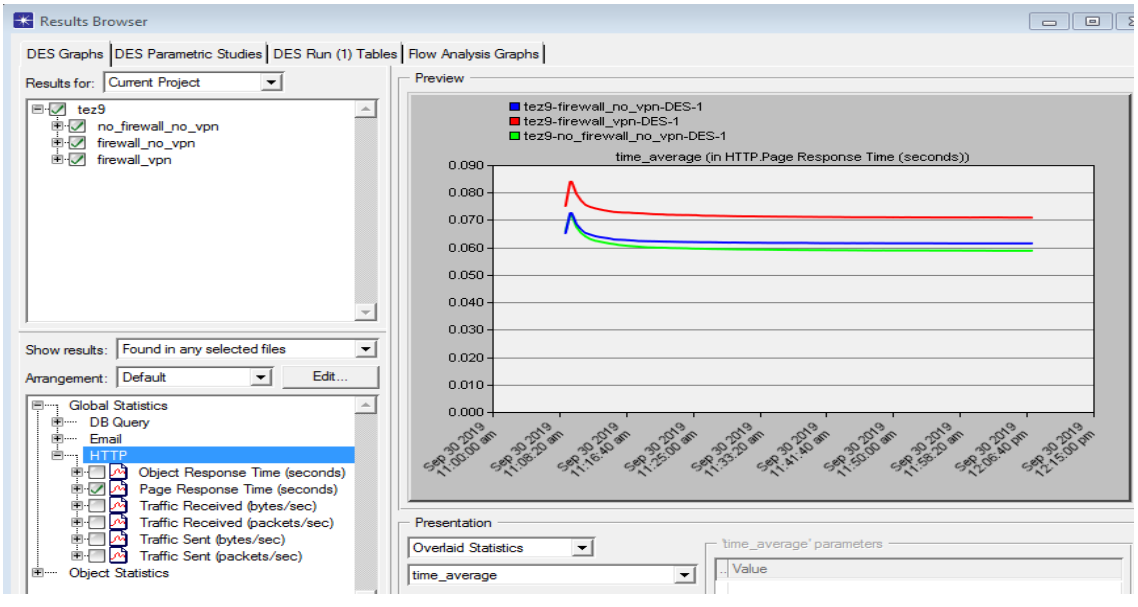
5.2.5. Benzetim İşleminin Başlatılması

Benzetim için hazırlanan üç senaryoda yapılan tüm işlemler kaydedilmiştir. Benzetim işlemi çalıştırma için Şekil 5.10'da görüldüğü gibi her senaryoyu sırayla çalıştıran ve her senaryo için tek bir ayar ortamı sunan **'Scenerios>Manage Scenerios'** menüsünden, her senaryo için 1 saatlik benzetim süresi seçilerek benzetimlerin süresi belirlenmiştir. **'Results'** başlığına tıklanarak **'collect all'** seçilerek tüm senaryolar için seçilen istatistik değerlerinin toplanması sağlanmıştır.



Şekil 5.10. İstatistik verilerini toplama için benzetimin başlangıç ayarları

Senaryolar için benzetim işlemleri sırası ile gerçekleştirilip bittikten sonra toplanan istatistik değerlerini ve oluşan grafikleri inceleme işlemi için yazılım menüsünden **'DES>Results>Compare Results...'** komutu ile Şekil 5.11'de görülen **Result Browser** penceresi açılarak istenilen senaryoya ve/veya senaryolara ait istatistik verilerine ait grafik çizimleri elde edilmiştir.



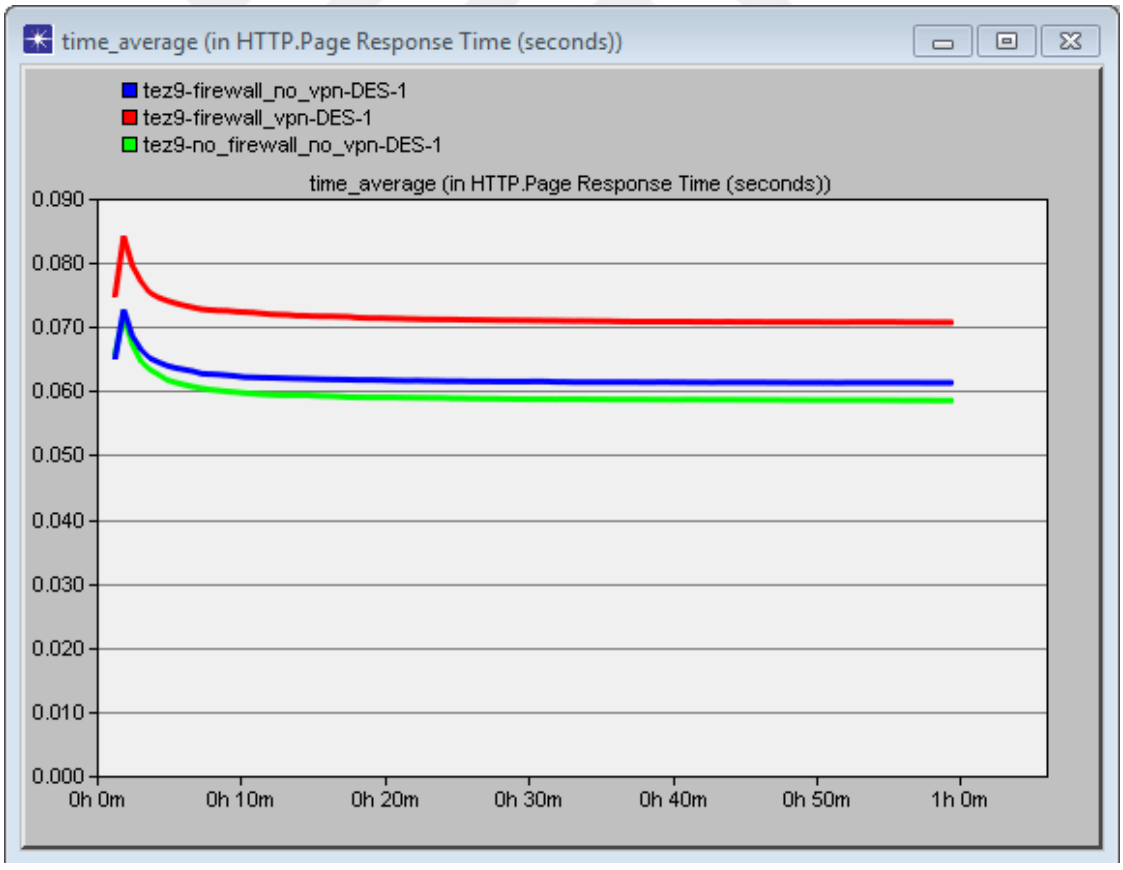
Şekil 5.11. Result Browser penceresi

5.3. Elde Edilen İstatik ve Grafikler

Benzetim sonrasında toplanan verilerin görselleştirilmesi işlemi senaryolar arasında yorum yapılmasına olanak sağlamıştır. Bu amaçla toplanan her istatistik ile ilgili grafiğin incelenmesi yapılarak benzetim sonuçları hakkında bir fikir edinilmiştir.

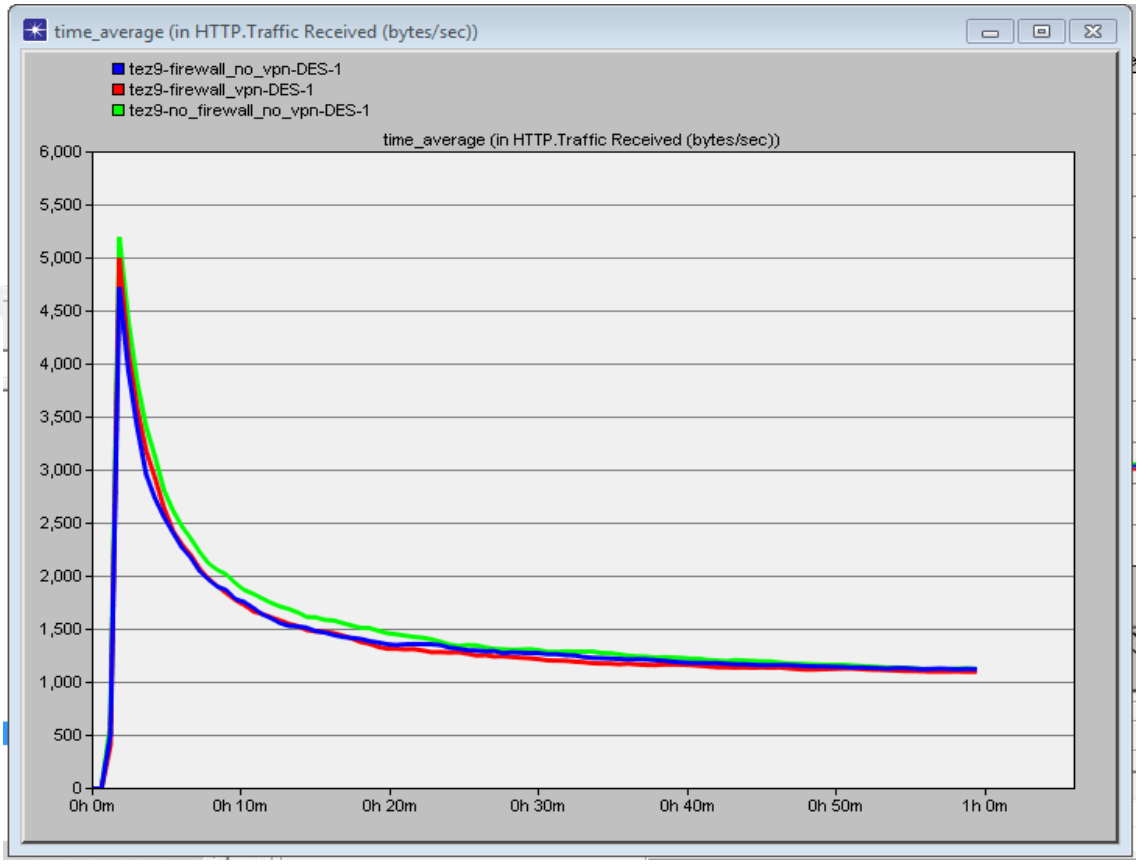
Benzetim işleminde dokuz adet istatistik verisi toplanmıştır. Üç senaryo için toplanan veriler tek bir grafik üzerinde gösterilerek karşılaştırma yapılması sağlanmıştır.

Şekil 5.12'de bir saat süresince süren benzetim işleminde bütün ağdaki istemcilerin web sunucudaki sayfalara ortalama erişim süreleri grafik halinde elde edilmiştir. "no_firewall_no_vpn" senaryosunda sayfa erişim sürelerinin en iyi olduğu gözlemlenmiştir. Burada en kötü performansın ortalama 10 ms farkla "Firewall_VPN" senaryosu olduğu açıkça gözlemlenmiştir. Sunucudan bir yanıt almak için geçen süreyi güvenlik duvarı ve sanal özel ağların etkilediğini göstermiştir. Grafik verileri *Ek-1*'de verilmiştir.



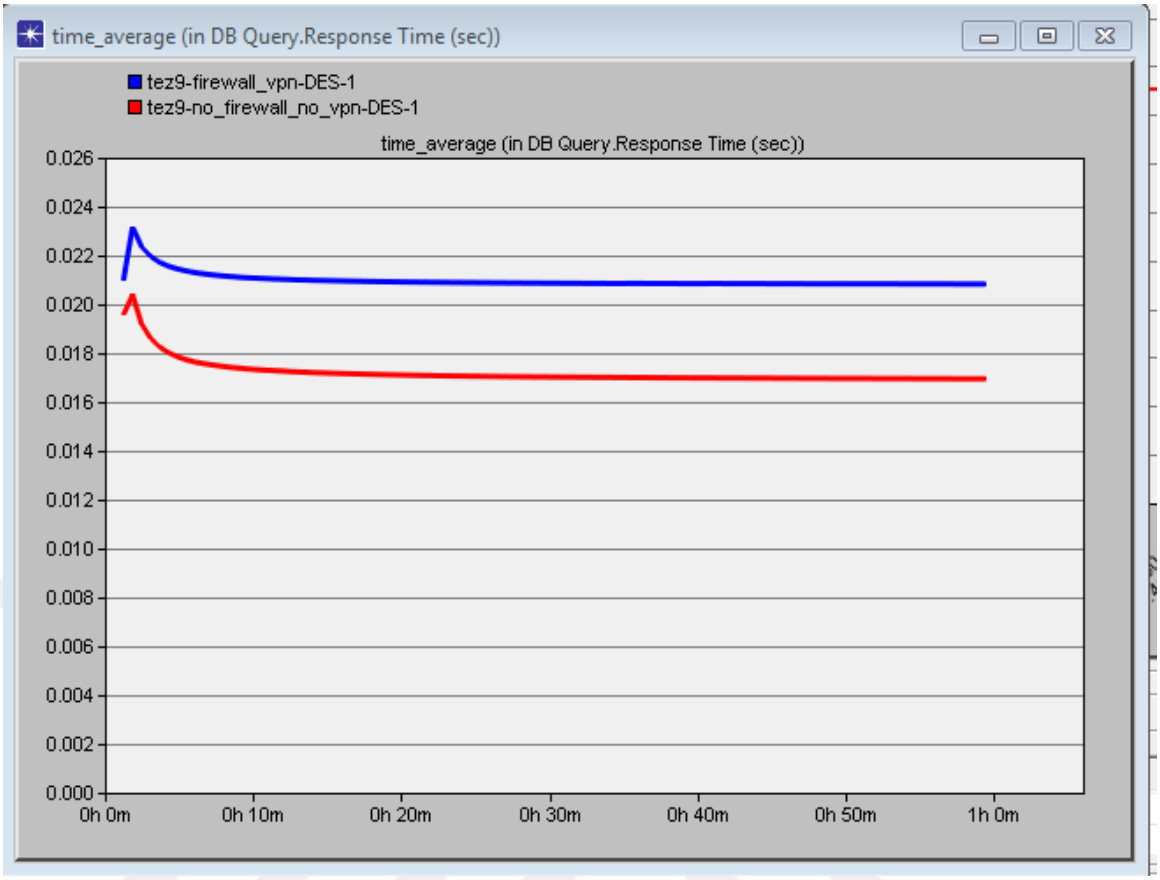
Şekil 5.12. HTTP sayfası yanıt süresi (saniye)

Şekil 5.13'te sunucu/istemci bilgisayarların http uygulamasından ortalama olarak saniye başına kaç bayt veri aldıkları gösterilmiştir. "no_firewall_no_vpn" senaryosu diğer iki senaryodan ortalama olarak saniye başına 150 bayt daha fazla veri alımı yapmıştır. Sunuculardan alınan veri miktarının güvenlik duvarı ve sanal özel ağların etkisi ile düştüğü gözlemlenmiştir. Grafik verileri *Ek-2*'de verilmiştir.



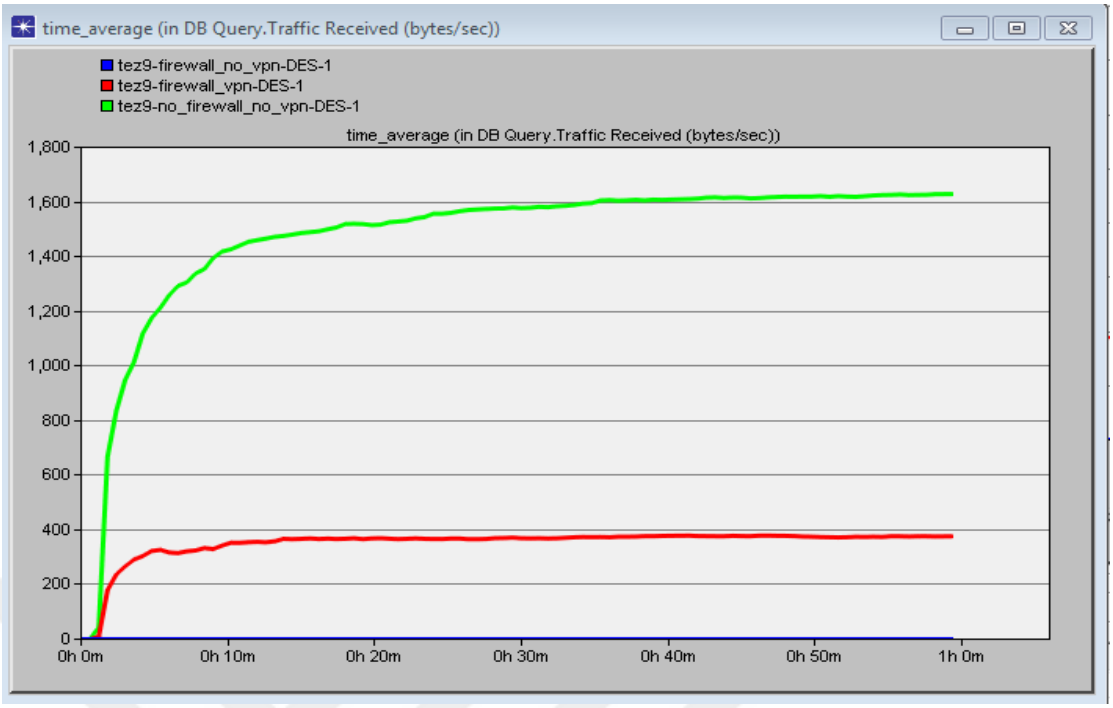
Şekil 5.13. HTTP Alınan Trafik (bayt/saniye)

Şekil 5.14'te ağdaki istemcilerin veri tabanı sunucusuna sql soruları için ortalama erişim süreleri grafik halinde elde edilmiştir. "firewall_no_vpn" senaryosunda Güvenlik Duvarında veri tabanı uygulamasına erişim engellendiği için veri toplanmamıştır. no_firewall_no_vpn" senaryosunda 4 ms daha iyi sonuç gözlemlenmiştir. Veri tabanına istemciler tarafından yapılan sorgulara yanıt süresindeki artışın sebebinin güvenlik duvarı ve sanal özel ağlar olduğu gözlemlenmiştir. Grafik verileri *Ek-3*'te verilmiştir.



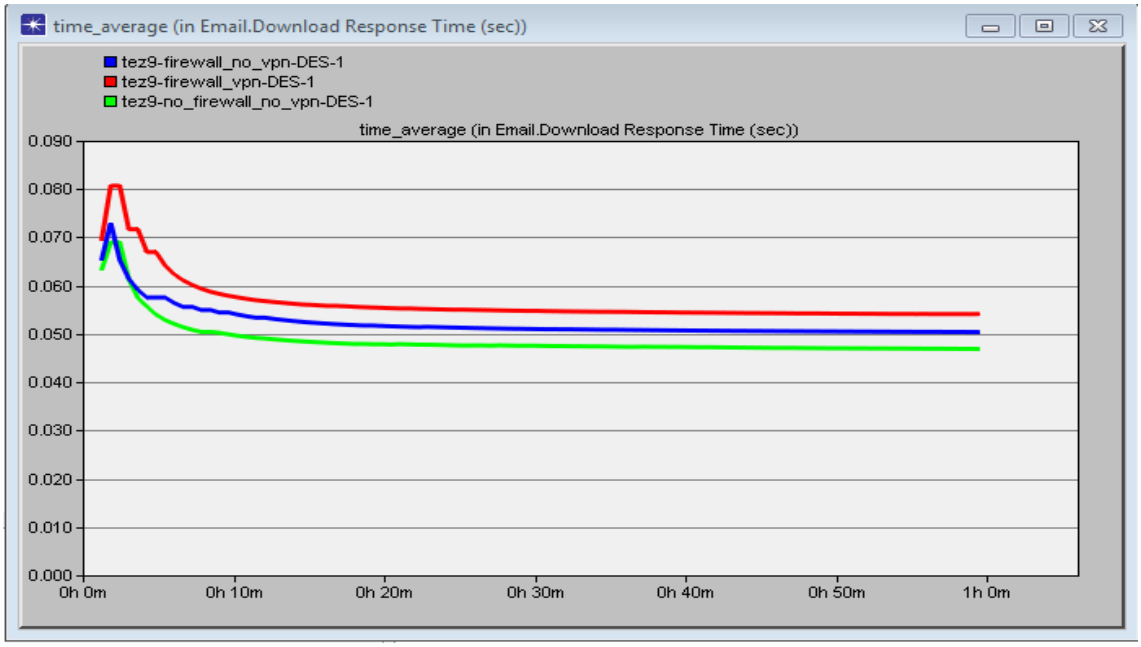
Şekil 5.14. DB Sorgusu Cevap Süresi (saniye)

Şekil 5.15'te benzetimdeki bilgisayarların ortalama saniye başına veri tabanı sorguları için aldıkları veri miktarı göstrerilmiştir. "firewall_no_vpn" senaryosunda Güvenlik Duvarında veri tabanı uygulamasına erişim engellendiği için veri toplanmamıştır. "no_firewall_no_vpn" senaryosunda "firewall_vpn" senaryosuna göre 1200 bayt daha iyi sonuç gözlemlenmiştir. Bu farkın sebebi, "firewall_vpn" senaryosunda sadece 'ra' yönlendiricisine bağlı 'sa' yerel alan ağı bölümündeki 200 bilgisayarın veri tabanı uygulamasına ulaşabilmesidir. Bununla beraber "no_firewall_no_vpn" senaryosunda ise bütün istemci bilgisayarlar veri tabanı uygulamasına ulaşabilmektedir. Bir veri tabanında örnek olarak; T.C. Kimlik numarası bilgisi 11 baytlık, ad/soyad bilgisi ise yaklaşık 50 baytlık bir hafıza alanında. Bu fark her T.C. Kimlik numarası ile ad/soyad bilgisini almak için yapılan bir sorguda, saniye başına 20 satırlık bir fark yaratır. Grafik verileri *Ek-4*'te verilmiştir.



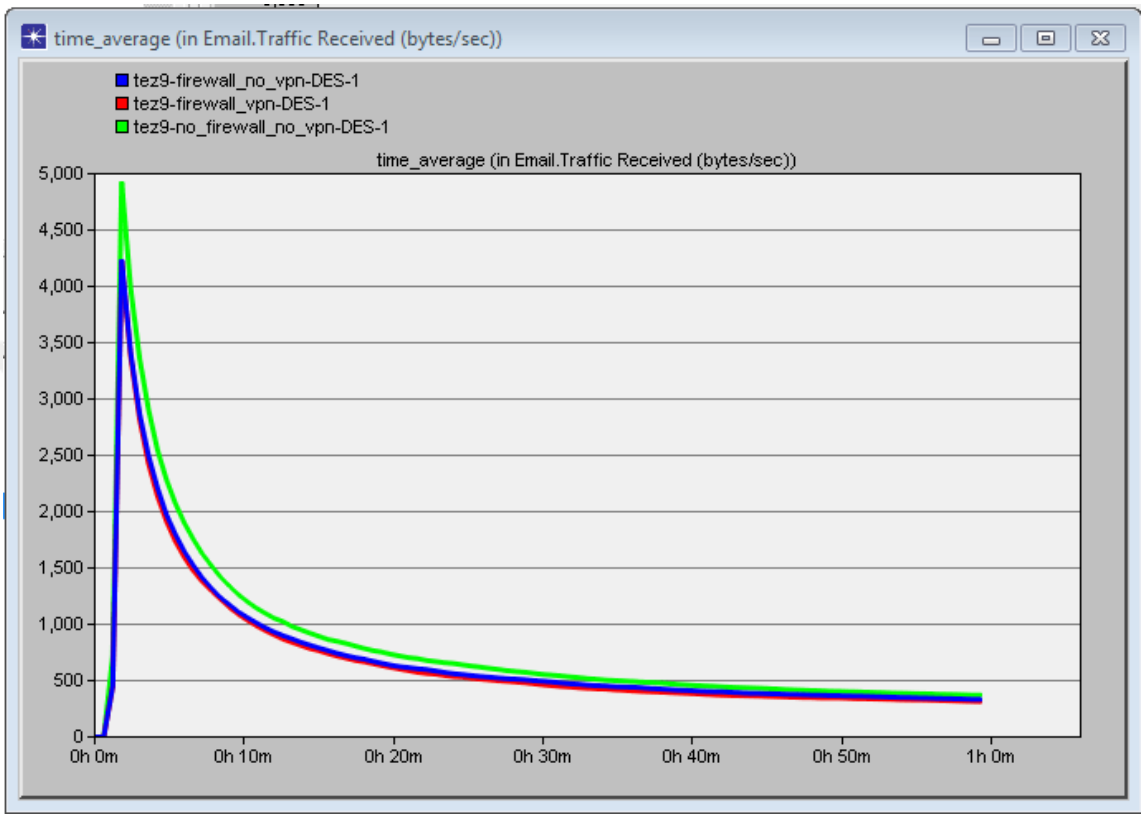
Şekil 5.15. DB Sorgusu Alınan Trafik (bayt/saniye)

Şekil 5.16'da E-posta indirme isteklerine verilen ortalama yanıt süreleri grafik halinde gösterilmiştir. "no_firewall_no_vpn" senaryosu "firewall_no_vpn" senaryosuna göre yaklaşık ortalama yaklaşık 3 ms, "firewall_vpn" senaryosuna göre ise ortalama yaklaşık 10 ms daha iyi bir yanıt süresi almıştır. Grafik verileri *Ek-5*'te verilmiştir Bu farklar ağ güvenliği uygulamalarının



Şekil 5.16. Eposta İndirme Yanıt Süresi (saniye)

Şekil 5.17'de benzetimdeki bilgisayarların ortalama saniye başına veri tabanı sorguları için aldıkları veri miktarı göstrerilmiştir. "no_firewall_no_vpn" senaryosunda "firewall_vpn" senaryosuna ve "firewall_no_vpn" senaryosuna göre sırasıyla 220 bayt ve 190 bayt daha iyi bir başarım göstermiştir. Grafik verileri *Ek-6*'da verilmiştir.

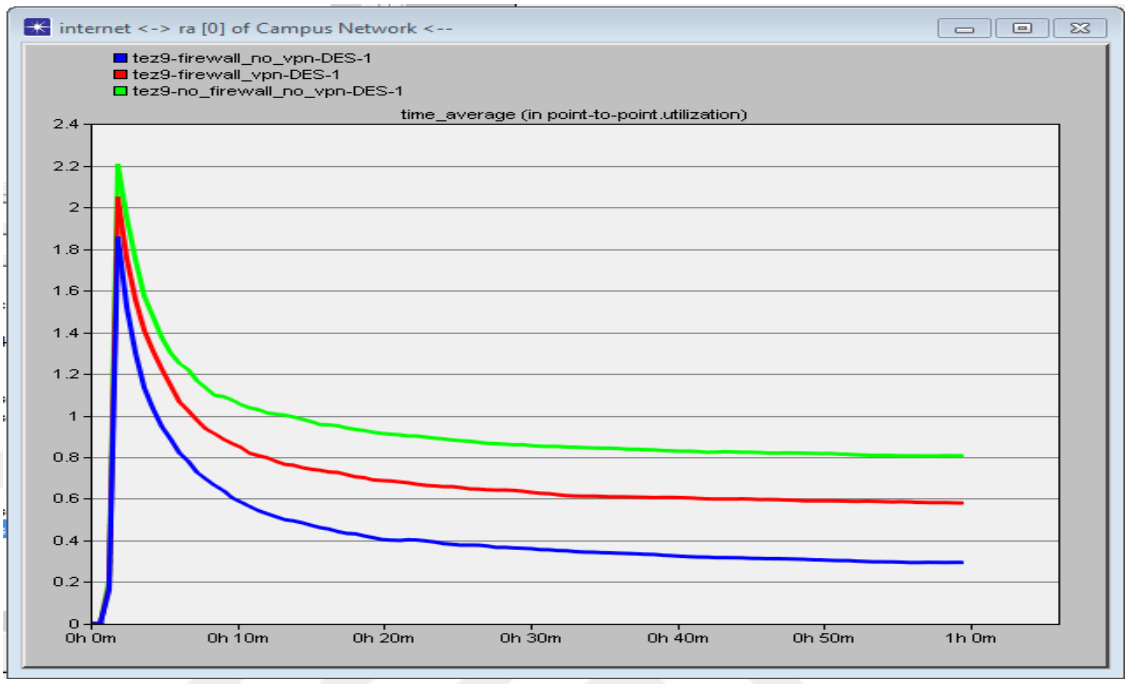


Şekil 5.17. Eposta Alınan Trafik (bayt/saniye)

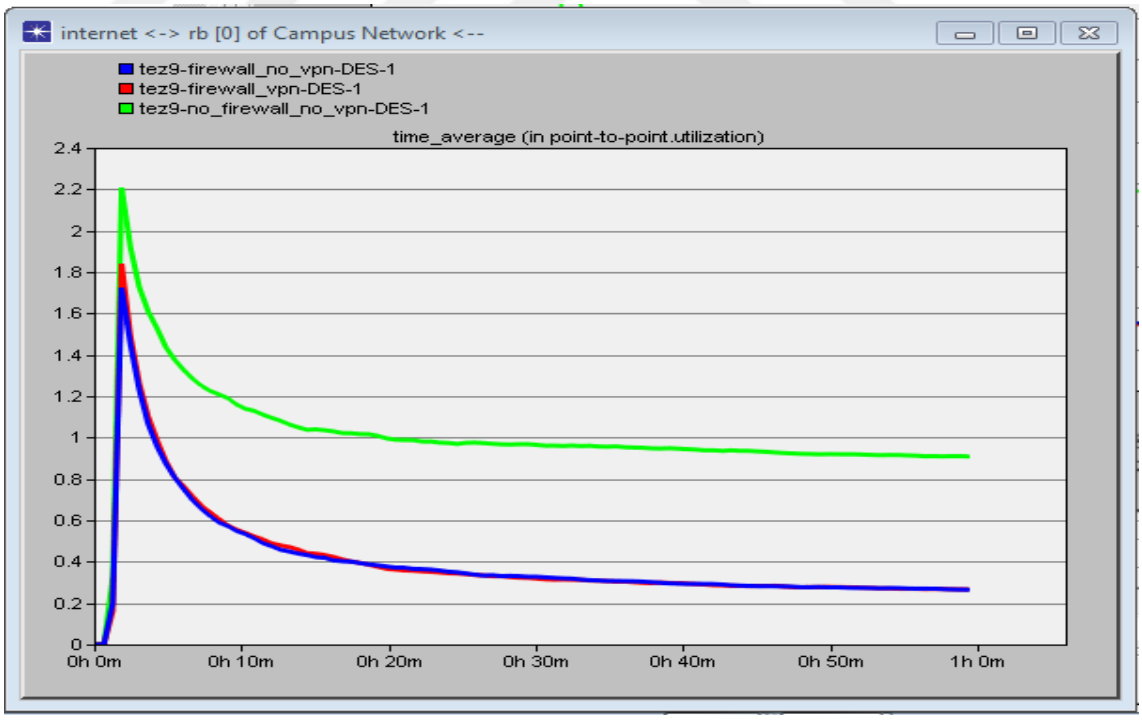
Şekil 5.18'de "internet" bulutu ile "ra" yönlendiricisi arasındaki DS1 linkinin, Şekil 5.19'da ise "internet" bulutu ile "rb" yönlendiricisi arasındaki DS1 linkinin kullanım oranları gösterilmiştir. Bu iki grafik arasındaki ilişki "ra" yönlendiricisinin "rd" yönlendiricisi arasında Sanal Özel Ağ Tüneli olmasıdır. Bundan dolayı her iki bağlantının kullanım oranları "firewall_vpn" senaryosunda farklılıklar göstermiştir.

Bu istatistik verilerinin farklı bir seri bağlantı üzerinde test etmek için DS1 bağlantıları E1 ile değiştirilmiş ve benzetim bu yapıda da çalıştırılmıştır. Şekil 5.20'de "internet" bulutu ile "ra" yönlendiricisi arasındaki bağlantı E1 linkinin, Şekil 5.21'de ise "internet" bulutu ile "rb" yönlendiricisi arasındaki E1 linkinin kullanım oranları gösterilmiştir. Bu iki grafik arasındaki ilişki "ra" yönlendiricisinin "rd" yönlendiricisi arasında Sanal Özel

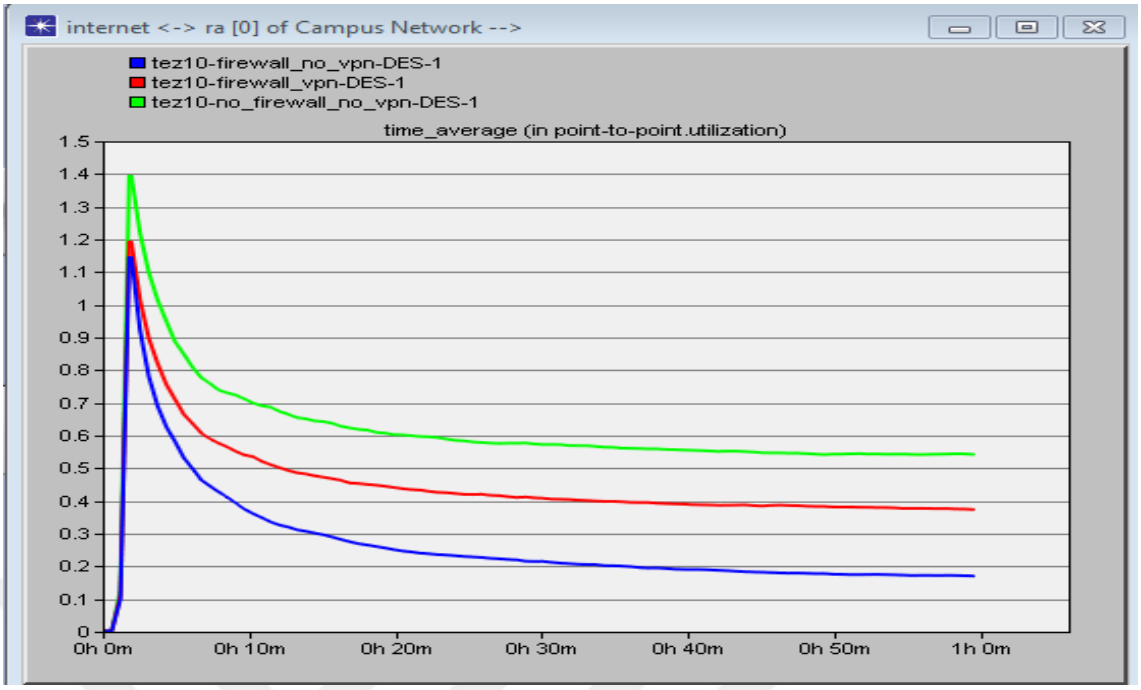
Ağ Tüneli olmasıdır. Bundan dolayı her iki bağlantının kullanım oranları “firewall_vpn” senaryosunda farklılıklar göstermiştir. Grafik verileri *Ek-7* ve *Ek-8*‘de verilmiştir.



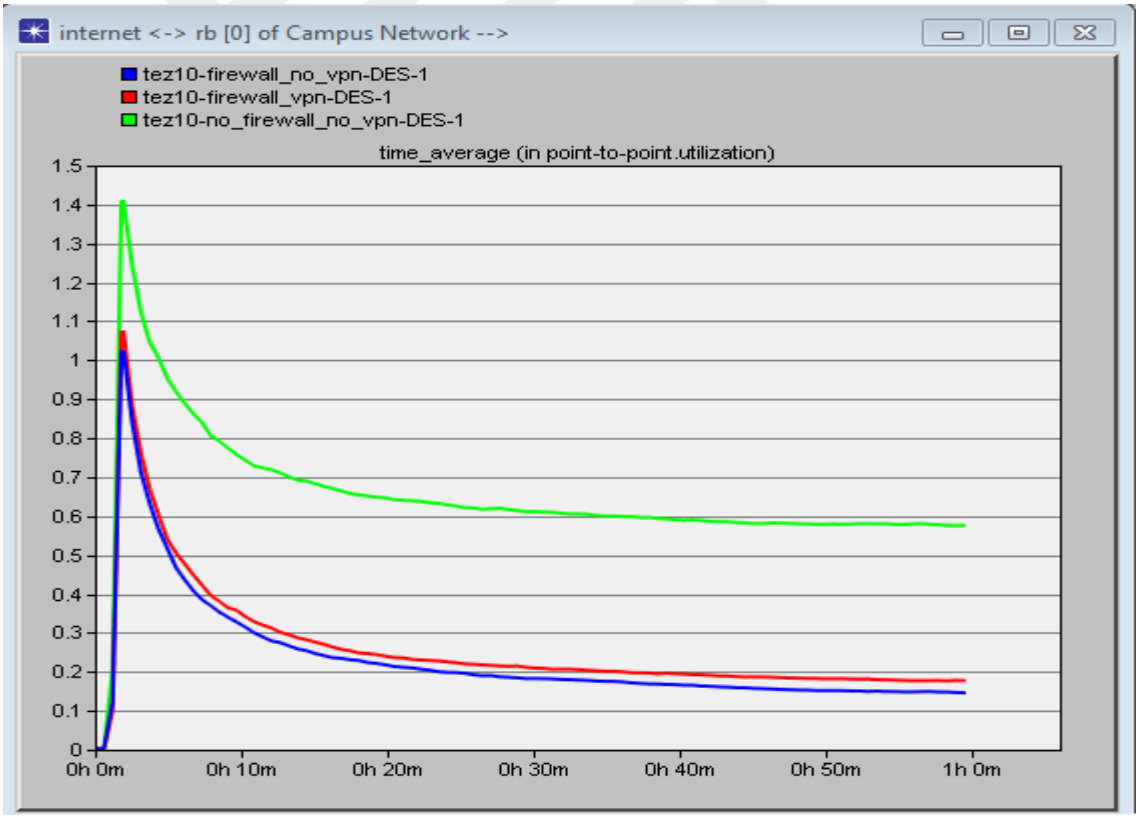
Şekil 5.18. internet – ra bağlantı kullanımı (DS1)



Şekil 5.19. internet – rb bağlantı kullanımı (DS1)

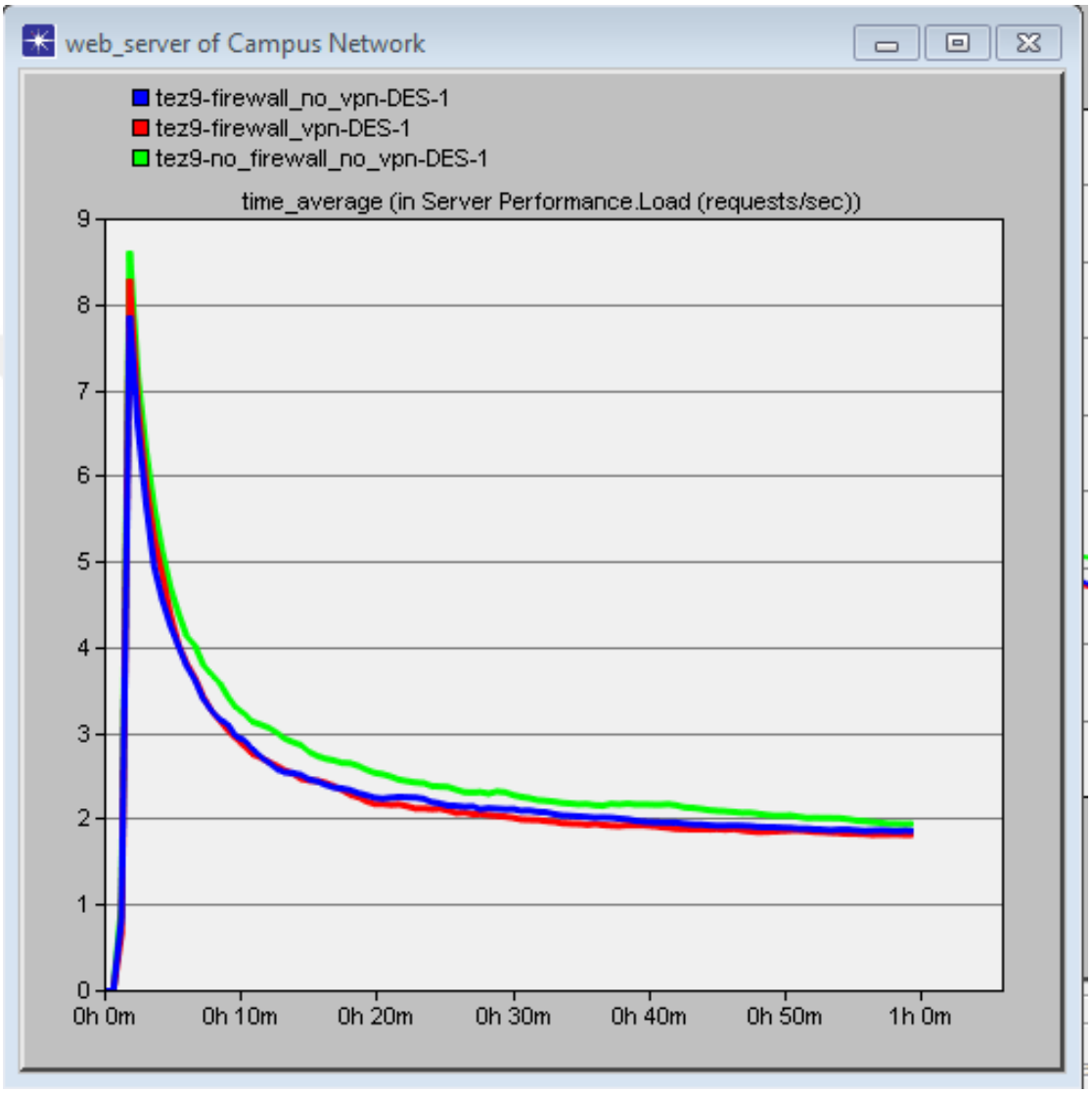


Şekil 5.20. internet – ra bağlantı kullanımı(E1)



Şekil 5.21. internet – rb bağlantı kullanımı(E1)

Şekil 5.22'de web sunucunun saniye başına ortalama işlem isteklerini grafik olarak göstermektedir. Grafik verilerine göre web sunucusu "no_firewall_no_vpn" senaryosunda diğer 2 senaryoya göre daha fazla istek almaktadır. Grafik verileri *Ek-9*'da verilmiştir.



Şekil 5.22. Sunucu Yük Performansı (istek/saniye)

BÖLÜM 6

SONUÇLAR ve TARTIŞMA

Güvenlik duvarları ve sanal özel ağlar, kuruluşların güvenlik ve uzaktan güvenli erişim ihtiyaçlarını sağlayan çözümler olarak neredeyse bir standart haline gelmiştir. Bilgisayar ağlarına uygulanan ek güvenlik tedbirlerinin ağ performansına ve başarımına olası etkileri vardır. Bu alanda daha önce yapılan çalışmalar incelendiğinde bu tarz etkilerin kaçınılmaz olduğu görülebilir. Var olan çalışmalar genelde bilgisayar ağlarının modellenmesi üzerinde durduğundan; elde edilen veriler ile güvenlik çözümlerinin ağ performansına olası etkilerini inceleyen bir yaklaşımın da olması gerekliliği vardır.

Bu çalışma, inceleme yapılan üç senaryo bakımından her iki güvenlik çözümünün ağ performansına etkilerini ayrı ayrı ortaya koymaktadır. Sanal özel ağ çözümünün aktif olduğu sistemlerde, istemcilerin uygulamalara gönderdiği isteklere olan yanıt sürelerinde çok büyük artışlara sebep olduğu görülmüştür. Güvenlik duvarı ve sanal özel ağın birlikte uygulandıkları sistemlerde istemcilerin yanıtlarında çok daha fazla gecikmeye sebep olmuştur.

Sanal özel ağlar ile güvenlik duvarlarının etkin olduğu güvenlik yapısında, uzak istemcideki herhangi bir uygulamaya sanal özel ağ üzerinden bağlantı yapan istemci ile sanal özel ağ üzerinden bağlanmayan istemci arasındaki fark incelemeye değerdir. Sanal özel ağ kullanan istemci kullanmayan istemciye göre internet bağlantı hattını daha yüksek oranda kullanmaktadır. Buna karşılık sanal özel ağ kullanan istemci kullanmayan istemciye göre saniye başına daha az veri alabilmektedir.

Senaryolar arasındaki farklar güvenlik duvarı ve sanal özel ağların ağ güvenliği için yaptığı işlemlerdir. Güvenlik duvarı uygulamasının uzak ağa ulaşmaya çalışan her paket için gerekli kuralları uygulaması sonucu ağda bir gecikme olduğu açıkça gözlemlenmiştir. Sanal özel ağ uygulaması ise, uçtan uca güvenilir bir bağlantı kurmak için iletişim için paketlere ek başlılar ekler. Bu iki uygulamanın da bant genişliğine ve işlem gecikmelerine sebep olduğu yapılan çalışmada bu etkiler elde edilen değerler ile ortaya koyulmuştur.

6.1. Katkıları

Kurumsal ağlarda güvenlik yaklaşımı birçok farklı model ve senaryo ile uygulanabilmektedir. Bu çalışmada uygulanan yöntemler, birçok farklı ağ yapısının performans analizi için kullanılabilir. Çalışma her ne kadar ağ performans analizi odaklı olsa da oluşturulacak ağ yapılarının modellenmesi ve test için bir yöntem içermektedir.

Günümüzde bir ağ alt yapısının tasarım ve kurulma maliyeti düşünüldüğünde, oluşturulan yapının isteklere cevap verip vermeyeceğini önceden kestirmek çok büyük bir önem arz etmektedir. Oluşturulacak ağ alt yapısının hangi seviyede güvenlik ihtiyacının olduğunu tespit etmekte bu açıdan yine çok önemlidir. Kurulum işleminden sonra ortaya çıkacak, ağdaki tıkanıklıklar ve dar boğazlar ile güvenlik ihtiyaçlarının bu durumlara olan olası yan etkilerini kestirebilmek büyük önem taşımaktadır. Bu yapılan çalışma ağ güvenliği ve ağ performansı dengesini kurmak için yapılacak ağ modellemeleri için bir yaklaşım sunmakta olup, literatürdeki diğer çalışmaları da destekler niteliktedir.

6.2. Öneriler

Bu çalışmada tek bir kurumsal ağ tipi üzerinde farklı senaryolar geliştirilmiştir. Fakat bundan sonraki çalışmalarda daha farklı ağ topolojileri üzerinde durulması daha farklı yaklaşımların ortaya çıkması için yardımcı olabilir. Ayrıca, güvenlik duvarı çözümü sadece uzak ağda uygulanmıştır. Bu anlamda istemci cihazlarında güvenlik duvarı çözümünün etkin olduğu bir senaryonun da olması daha gerçekçi bir yaklaşım sağlayabilir.

Bu çalışmadaki bütün işlemler benzetim ortamında gerçekleştirilmiştir. Her ne kadar benzetim ortamlarının gerçek dünya uygulamalarına çok yakın sonuçlar çıkardığı bilinse de uygulamanın gerçek bir kurumsal ağ yapısında performans ölçen yazılımlar ile gerçekleştirilmesi, benzetim ortamları ile gerçek uygulama arasındaki farklılık ve benzerlikleri gözlemlemek açısında yararlı olabilir.

Geliştirilen benzetim ortamı tamamen IPv4 ağları göz önüne alınarak tasarlanmıştır. Yakın bir gelecekte IPv6 hayatımızın kaçınılmaz bir parçası olacaktır. IPv6 ağlarının güvenlik istekleri farklılıklar göstermektedir. Bu ve bunun gibi çalışmaların IPv6 ağları İçinde gerçekleştirilmesi geleceğe hazırlanmak açısından yarar sağlayabilir.

Günümüzün çok sık kullanılan çeşitli sanallaştırma araçları ile benzeri bir çalışma, benzetim yerine öykünme yöntemi kullanılarak da yapılabilir. Bu tür bir çalışma sanallaştırma işlemi ile gerçek donanımlar arasındaki farkı analiz etmek için yararlı olabilir.

KAYNAKLAR

Agbenyegah, F. K., & Asante, M. (2017). Impact Of Firewall On Network Performance. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, *6*(03), 32–38.

Ahmed, A. A. H. (2009). Modeling Computer Laboratories in University that Contains Eight Colleges by Using OPNET Software. *Journal of Kerbala University*, *7*(1), 108–123.

Ahmed, S. E. M., & Mustafai, A. B. A. (2015). The Impact of Security Overhead Traffic on Network's Resources Performance. *IOSR Journal of Computer Engineering*, *17*(1), 79–84. https://doi.org/10.9790/0661-17127984

Akbaş, D., & Gümüşkaya, H. (2011). Real and OPNET modeling and analysis of an enterprise network and its security structures. *Procedia Computer Science*, *3*, 1038–1042. https://doi.org/10.1016/j.procs.2010.12.170

Alpern, N. J., & Shimonski, R. J. (2010). Network Fundamentals. İçinde *Eleventh Hour Network+* (ss. 1–18). https://doi.org/10.1016/b978-1-59749-428-1.00003-5

Aydın, E. D. (2012). AĞ GÜVENLİĞİ. *İstanbul Üniversitesi İletişim Fakültesi Dergisi | Istanbul University Faculty of Communication Journal*, 0(6), 43–59. https://doi.org/10.17064/iüifhd.34467

Bıyan, M., & Alan, M. A. (2013). Cumhuriyet Üniversitesi Bilgisayar Ağının Modellenmesi ve Uzaktan Eğitim için Performans Ölçümü. *Sosyal Bilimler Araştırmaları Dergisi*, *8*(2), 99–111. https://dergipark.org.tr/en/pub/gopsbad/issue/48564/616684

Çakır, C., & Kaptan, H. (2009). VoIP Teknolojilerinde Opnet Tabanlı Güvenlik Uygulaması. *Bilişim Teknolojileri Dergisi*, *2*(3), 1–7.

Can, Ö., & Akbaş, M. F. (2014). KURUMSAL AĞ VE SİSTEM GÜVENLİĞİ POLİTİKALARININ ÖNEMİ VE BİR DURUM ÇALIŞMASI. *TUBAV Bilim Dergisi*, *7*(2), 16–31.

Cerf, V. G., & Kahn, R. E. (1974). A Protocol for Packet Network Intercommunication. İçinde *IEEE Trans on Comms*.

Chang, X. (1999). Network simulations with OPNET. *WSC'99. 1999 Winter Simulation Conference Proceedings. "Simulation - A Bridge to the Future" (Cat. No.99CH37038)*, *1*, 307–314. https://doi.org/10.1109/WSC.1999.823089

Chen, M., Miao, Y., & Humar, I. (2019). Introduction to OPNET Network Simulation. İçinde *OPNET IoT Simulation* (ss. 77–153). https://doi.org/10.1007/978-981-32-9170-6_2

Comer, D. E. (2009). *Computer Networks and Internets* (Fifth; M. J. Horton, Ed.). New Jersey: Pearson.

Davie, B. S., & Farrel, A. (2008). Virtual Private Networks. İçinde *MPLS: Next Steps* (ss. 351–369). https://doi.org/10.1016/B978-0-12-374400-5.00012-6

Day, J. D., & Zimmermann, H. (1983). The OSI Reference Model. *Proceedings of the IEEE*, *71*(12), 1334–1340. https://doi.org/10.1109/PROC.1983.12775

Develi, H. (2009). *Süleyman Demirel Üniversitesi kampüs ağının OPNET ile Modellenmesi*. Süleyman Demirel Üniversitesi/Fen Bilimleri Enstitüsü, Isparta.

Dostálek, L., & Kabelová, A. (2006). *Understanding TCP/IP A clear and comprehensive guide to TCP/IP protocols*.

Dubrawsky, I. (2010). Network Security. İçinde *Eleventh Hour Security+* (ss. 61–76). https://doi.org/10.1016/B978-1-59749-427-4.00005-8

Durkaya, A. K., Bascil, M. S., & Er, O. (2011). A System Design: Purposed of Data Transmission and Far Control using IPv6 Internet Protocol. *Electronic Letters on Science & Engineering*, *7*(1), 1–7

Faircloth, J. (2014). Networks. İçinde *Enterprise Applications Administration* (ss. 27–79). https://doi.org/10.1016/B978-0-12-407773-7.00002-8

Fırlar, T. (2003). Ağ Güvenliği. *SAÜ Fen Bilimleri Enstitüsü Dergisi*, *7*(1), 9–16. https://doi.org/10.16984/saufbed.39608

Fulp, E. W. (2013). Firewalls. İçinde *Managing Information Security: Second Edition* (ss. 143–175). https://doi.org/10.1016/B978-0-12-416688-2.00006-4

Gallo, M. A., & Hancock, W. M. (2002a). Fundamental Concepts of Computer Networks and Networking. İçinde *Networking Explained* (ss. 1–29). https://doi.org/10.1016/b978-155558252-4/50027-4

Gallo, M. A., & Hancock, W. M. (2002b). The Internet and TCP/IP. İçinde *Networking Explained* (ss. 55–138). https://doi.org/10.1016/b978-155558252-4/50029-8

Goralski, W. (2017a). Firewalls. İçinde *The Illustrated Network* (ss. 799–812). https://doi.org/10.1016/B978-0-12-811027-0.00032-1

Goralski, W. (2017b). TCP/IP Protocols and Devices. İçinde *The Illustrated Network* (ss. 47–69). https://doi.org/10.1016/b978-0-12-811027-0.00002-3

Gürtürk, U., & Daş, R. (2017). Ağ Benzetim ve Modelleme Araçlarının İncelenmesi. *Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi*, *17*(2), 516–536. https://dergipark.org.tr/tr/pub/akufemubid/issue/43399/524726

Harmening, J. T. (2017). Virtual Private Networks. İçinde *Computer and Information Security Handbook* (ss. 843–856). https://doi.org/10.1016/B978-0-12-803843-7.00058-2

Hofmann, M., & Beaumont, L. (2005). Building Content Networks. İçinde *Content Networking* (ss. 263–278). https://doi.org/10.1016/b978-155860834-4/50028-7

Kale, C. J., & Socolofsky, T. J. (1991). TCP/IP tutorial. *RFC 1180*

Kartal, M., Sağiroğlu, Ş., & Bülbül, H. İ. (2013). IPV6'da Güvenlik Açıklarına Genel Bir Bakış. *Politeknik Dergisi*, *16*(3), 119–127. https://doi.org/10.2339/2013.16.3

Kenyon, T. (2002). Network design and modeling. İçinde *High Performance Data Network Design* (ss. 91–141). https://doi.org/10.1016/b978-155558207-4/50004-5

Khaleel Hasan, M. (2017). *Farklı Ağ Teknolojilerinde Trafik Ölçümü ve Performans Karşılaştırması*. Erciyes Üniversitesi Fen Bilimleri Enstitüsü.

Kocabaş, E. (2019). *IPv4 ve IPv6 Desteklenen Yönlendirme Protokollerinin Performans Analizi / Karşılaştırılması*. Karabük Üniversitesi/Fen Bilimleri Enstitüsü, Karabük.

Krit, S., & Haimoud, E. (2017). Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically. *2017 International Conference on Engineering & MIS (ICEMIS)*, 1–7. https://doi.org/10.1109/ICEMIS.2017.8273003

Kumar, K. M. K., & Bakon, K. A. (2015). The Analysis of Firewall and VPN in Enterprise Network Performances. *International Journal of Information Systems and Engineering*, *3*(1), 129–150. https://doi.org/10.24924/ijise/2015.11/v3.iss1/129.150

Kurose, J. F., & Ross, K. W. (2013). Computer Networking A Top-Down Approach. İçinde *Computer* (Sixth).

Lawal, I. A., Said, A. M., Mu'azu, A. A., & Shah, P. A. (2014). Performance Comparison of Centralized and Distributed Network Models to Support QoS in Fixed WiMAX. *Procedia - Social and Behavioral Sciences*, *129*, 441–452. https://doi.org/10.1016/j.sbspro.2014.03.699

Li, Y., Li, D., Cui, W., & Zhang, R. (2011). Research based on OSI model. *2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011*, 554–557. https://doi.org/10.1109/ICCSN.2011.6014631

Lloyd, D. (2001). TCP/IP and the OSI Model. İçinde J. Wheat, R. Hiser, J. Tucker, A. Neely, & A. McCullough (Ed.), *Designing A Wireless Network* (ss. 73–114). https://doi.org/10.1016/B978-192899445-9/50008-X

Lu, Z., & Yang, H. (2012). *Unlocking the Power of OPNET Modeler*. Cambridge: Cambridge University Press

Mackay, S., Wright, E., Reynders, D., & Park, J. (2004). TCP/IP overview. İçinde *Practical Industrial Data Networks* (ss. 257–276). https://doi.org/10.1016/b978-075065807-2/50040-6

Madan, A., & Bharti, A. T. (2014). OSI Reference Model. İçinde *International Journal of Advanced Research in Computer Science and Software Engineering* (C. 4).

Makasiranondh, W., Maj, S. P., & Veal, D. (2010). Pedagogical evaluation of simulation tools usage in Network Technology Education. *World Transactions on Engineering and Technology Education*, *8*(3), 321–326.

Malik, A., & Verma, H. K. (2012). Performance Analysis of Virtual Private Network for Securing Voice and Video Traffic. *International Journal of Computer Applications*, *46*(16), 25–30.

Melendez, W. A. (1999). The upper layers of the ISO/OSI Reference Model (Part II). *Computer Standards and Interfaces*, *20*(4–5), 185–199. https://doi.org/10.1016/S0920-5489(98)00057-9

Mohorko, J., Fras, M., & Klampfer, S. (2008). Advanced modelling and simulation methods for communication networks. *Mikrotalasna revija*.

Nalbatcı, İ., Bayılmış, C., İskefiyeli, M., & Kırbaş, İ. (2013). WiMAX Ağlarda Çoklu Ortam Trafiklerinin OPNET Kullanarak Başarım Analizi. *APJES*, *1*(3), 26–40. https://doi.org/10.5505/apjes.2013.21931

Pala, Z. (2017). Kampüs Ağlarında Arkaplan Trafiğin IP-Tabanlı Telefon Sistemlerin Ses Kalitesi Üzerindeki Etkisi The Impact of the Background Traffic on the IP-Based Phone Systems Sound Quality in the Campus Network. *Fen Bilimleri Enst. Der. / Iğdır Univ. J. Inst. Sci. & Tech*, *7*(2), 55–63. https://doi.org/10.21597/jist.2017.140

Plummer, D. (1982). An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. *RFC 826* https://tools.ietf.org/html/rfc826

Postel, J. (1981a). Internet Control Message Protocol. *RFC 792* https://tools.ietf.org/html/rfc792

Postel, J. (1981b). Internet Protocol. *RFC 791* https://tools.ietf.org/html/rfc791

Postel, J., & Reynolds, J. K. (1983). Assigned numbers. *RFC 870* https://tools.ietf.org/html/rfc870

Rahman, M. A., Pakštas, A., & Wang, F. Z. (2009). Network modelling and simulation tools. *Simulation Modelling Practice and Theory*, *17*(6), 1011–1031. https://doi.org/10.1016/j.simpat.2009.02.005

Reynders, D., Mackay, S., Wright, E., & Mackay, S. (2004). TCP/IP overview. İçinde *Practical Industrial Data Communications* (ss. 112–126). https://doi.org/10.1016/b978-075066395-3/50010-3

Shinder, L. (2000). TCP/IP Overview. İçinde *Troubleshooting Windows 2000 TCP/IP* (ss. 1–49). https://doi.org/10.1016/B978-192899411-4/50004-3

Shinder, T. W. (2007). Configuring Virtual Private Networking. İçinde *The Best Damn Firewall Book Period* (ss. 539–577). https://doi.org/10.1016/b978-1-59749-218-8.00016-8

Stallings, W. (2011). *NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS FOURTH EDITION* (Fourth; M. J. Horton, H. Michael, T. Dunkelberger, M. Haggerty, & A. Michael, Ed.). New Jersey: Pearson.

Suárez, F. J., Nuño, P., Granda, J. C., & García, D. F. (2015). Computer networks performance modeling and simulation. İçinde M. S. Obaidat, P. Nicopolitidis, & F. Zarai (Ed.), *Modeling and Simulation of Computer Networks and Systems* (ss. 187–223). https://doi.org/10.1016/B978-0-12-800887-4.00007-9

Sütçü, C. (2014). Bilgisayar ve Bilgisayar Ağları. *Marmara İletişim Dergisi*, *5*(5), 145–152.

Svensson, T., & Popescu, A. (2003). *OPNET Modeler Development of laboratory exercises based on OPNET Modeler*. Blekinge Institute of Technology.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *COMPUTER NETWORKS*. Boston: Pearson.

Üstündağ, D. T. (2009). *Comperative Routing Performance Analysis Of IPv4 And IPv6*. Atilim Univercity,İstanbul.

Vacca, J. R., & Ellis, S. R. (2005). Firewall Types. İçinde *Firewalls* (ss. 49–57). https://doi.org/10.1016/B978-155558297-5/50005-0

W. Shinder, T., Shinder, D. L., Shimonski, R. J., Hourihan, K. X., Stanger, J., Cook, R., & Amon, C. (2003). Firewall Concepts. İçinde A. Carasik-Henmi, T. W. Shinder, & D. L. Shinder (Ed.), *The Best Damn Firewall Book Period* (ss. 53–71). https://doi.org/10.1016/B978-193183690-6/50043-1

Yüksel, E., & Örencik, B. SANAL ÖZEL AĞ TASARIMI VE GERÇEKLEMESİ. 12 Ekim 2019 tarihinde http://www.emo.org.tr/ekler/d5c5e1c04111451_ek.pdf adresinden erişildi.

Zaballos, A., Corral, G., Serra, I., & Abella, J. (2003). Testing Network Security Using OPNET. İçinde *Opnetwork 2003*. Washington D.C.

Zararlı yazılımların 1984-2018 arası artışı (2018). 18 Mayıs 2018 tarihinde https://www.av-test.org/en/statistics/malware adresşnden erişildi.

Zimmermann, H. (1980). OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, *28*(4), 425–432. https://doi.org/10.1109/TCOM.1980.1094702

EKLER

Ek-1 http Sayfa Yanıt Süresi Grafiğine Ait İstatistik Verileri

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
0	#N/A	#N/A	#N/A
36	#N/A	#N/A	#N/A
72	0,065146	0,074986	0,065877
108	0,072866	0,084284	0,072190
144	0,068762	0,079724	0,067658
180	0,066635	0,077247	0,065428
216	0,065279	0,075495	0,063989
252	0,064670	0,074757	0,063050
288	0,064117	0,074251	0,062454
324	0,063747	0,073842	0,062104
360	0,063500	0,073492	0,061760
396	0,063252	0,073191	0,061418
432	0,062871	0,072910	0,061191
468	0,062786	0,072783	0,060872
504	0,062724	0,072688	0,060708
540	0,062606	0,072669	0,060529
576	0,062488	0,072526	0,060403
612	0,062316	0,072457	0,060275
648	0,062279	0,072392	0,060133
684	0,062243	0,072242	0,060001
720	0,062215	0,072122	0,059965

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
756	0,062180	0,072067	0,059899
792	0,062131	0,072031	0,059897
828	0,062096	0,071899	0,059838
864	0,062069	0,071888	0,059761
900	0,062021	0,071823	0,059741
936	0,061990	0,071800	0,059705
972	0,061959	0,071800	0,059670
1008	0,061942	0,071760	0,059582
1044	0,061919	0,071734	0,059544
1080	0,061882	0,071590	0,059521
1116	0,061871	0,071532	0,059486
1152	0,061869	0,071524	0,059438
1188	0,061848	0,071514	0,059414
1224	0,061803	0,071467	0,059390
1260	0,061775	0,071446	0,059357
1296	0,061760	0,071398	0,059334
1332	0,061780	0,071362	0,059301
1368	0,061743	0,071329	0,059274
1404	0,061730	0,071322	0,059244
1440	0,061703	0,071308	0,059247
1476	0,061680	0,071306	0,059225
1512	0,061694	0,071274	0,059211
1548	0,061653	0,071249	0,059197
1584	0,061648	0,071242	0,059179
1620	0,061640	0,071221	0,059151
1656	0,061638	0,071202	0,059115
1692	0,061624	0,071185	0,059115
1728	0,061633	0,071185	0,059091
1764	0,061634	0,071168	0,059067
1800	0,061637	0,071157	0,059056
1836	0,061648	0,071136	0,059041
1872	0,061631	0,071128	0,059035
1908	0,061579	0,071121	0,059015
1944	0,061575	0,071094	0,059014
1980	0,061542	0,071075	0,059020
2016	0,061539	0,071080	0,059001

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
2052	0,061537	0,071069	0,058979
2088	0,061536	0,071045	0,058970
2124	0,061532	0,071046	0,058968
2160	0,061528	0,071006	0,058970
2196	0,061529	0,070993	0,058946
2232	0,061531	0,070977	0,058941
2268	0,061522	0,070969	0,058921
2304	0,061517	0,070975	0,058904
2340	0,061530	0,070971	0,058893
2376	0,061529	0,070971	0,058873
2412	0,061512	0,070977	0,058882
2448	0,061509	0,070973	0,058884
2484	0,061498	0,070962	0,058881
2520	0,061496	0,070945	0,058879
2556	0,061484	0,070946	0,058883
2592	0,061491	0,070940	0,058874
2628	0,061493	0,070953	0,058878
2664	0,061502	0,070940	0,058874
2700	0,061496	0,070934	0,058866
2736	0,061493	0,070933	0,058866
2772	0,061489	0,070925	0,058865
2808	0,061487	0,070919	0,058856
2844	0,061474	0,070919	0,058856
2880	0,061468	0,070915	0,058852
2916	0,061461	0,070912	0,058850
2952	0,061451	0,070914	0,058844
2988	0,061454	0,070911	0,058847
3024	0,061450	0,070906	0,058839
3060	0,061451	0,070906	0,058827
3096	0,061447	0,070893	0,058828
3132	0,061454	0,070908	0,058824
3168	0,061453	0,070923	0,058817
3204	0,061453	0,070920	0,058814
3240	0,061455	0,070922	0,058804
3276	0,061452	0,070911	0,058784
3312	0,061454	0,070918	0,058787

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
3348	0,061456	0,070895	0,058783
3384	0,061455	0,070872	0,058789
3420	0,061458	0,070871	0,058774
3456	0,061435	0,070873	0,058772
3492	0,061435	0,070865	0,058770
3528	0,061437	0,070868	0,058777
3564	0,061438	0,070860	0,058773
3600	#N/A	#N/A	#N/A

Ek-2 http Alınan Trafik Grafiğine Ait İstatistik Verileri

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
0	0,000000	0,000000	0,000000
36	0,000000	0,000000	0,000000
72	511,259259	406,694444	603,055556
108	4720,888889	4993,513889	5217,902778
144	3947,050000	4115,888889	4336,638889
180	3405,828704	3579,453704	3818,958333
216	2961,650794	3184,142857	3417,345238
252	2733,496528	2925,760417	3102,357639
288	2559,373457	2645,728395	2847,391975
324	2413,177778	2431,052778	2666,163889
360	2273,037879	2302,815657	2507,575758
396	2175,192130	2202,620370	2438,064815
432	2047,959402	2072,508547	2307,694444
468	1967,305556	1977,079365	2236,392857
504	1902,701852	1906,935185	2181,262963
540	1871,701389	1838,036458	2082,442708
576	1785,477124	1775,683007	2002,339869
612	1758,041667	1729,038580	1965,037037
648	1703,099415	1669,412281	1902,422515

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
684	1643,605556	1645,586111	1881,783333
720	1604,525132	1614,076720	1859,596561
756	1559,185606	1585,181818	1825,914141
792	1534,094203	1553,150966	1781,044686
828	1528,423611	1529,862269	1758,160880
864	1515,194444	1493,110000	1736,580000
900	1483,981838	1481,436966	1690,448718
936	1470,660494	1478,307613	1660,833333
972	1447,315476	1465,509921	1640,718254
1008	1429,262452	1443,003831	1629,611111
1044	1420,939815	1414,429630	1612,812963
1080	1411,058244	1381,819892	1609,568996
1116	1389,664931	1363,837674	1591,290799
1152	1376,736532	1334,956229	1564,696128
1188	1360,515523	1317,322712	1541,918301
1224	1352,938889	1317,246825	1532,273810
1260	1359,322531	1312,083333	1514,765432
1296	1362,352102	1313,940691	1492,928679
1332	1361,028509	1301,134503	1482,013158
1368	1359,866809	1285,153846	1472,718661
1404	1351,455556	1286,263194	1469,469444
1440	1328,032520	1282,118564	1449,130759
1476	1317,782407	1285,059524	1445,527778
1512	1303,852067	1270,822997	1443,620801
1548	1301,376263	1253,361111	1425,232323
1584	1294,157407	1256,730864	1407,440123
1620	1295,917874	1244,585749	1404,373188
1656	1276,984043	1246,265957	1407,034279
1692	1283,084491	1239,131366	1396,800926
1728	1280,247166	1232,248866	1412,531746
1764	1276,602222	1228,103889	1406,235556
1800	1276,512527	1219,728758	1386,539760
1836	1266,441774	1207,831731	1373,608974
1872	1266,835430	1205,989518	1364,754193
1908	1257,433128	1203,932613	1350,493827
1944	1254,765152	1196,247475	1346,006566

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
1980	1240,682540	1191,091766	1339,772321
2016	1231,489279	1181,150097	1330,441033
2052	1229,244253	1178,400862	1326,963602
2088	1225,472222	1177,531073	1321,562618
2124	1222,291667	1171,702778	1322,881944
2160	1216,503188	1177,059199	1314,645719
2196	1218,500448	1169,322581	1311,126792
2232	1216,960317	1165,718254	1324,121693
2268	1210,498698	1163,393663	1320,027344
2304	1205,573504	1168,736325	1323,917094
2340	1195,449074	1168,453704	1319,294613
2376	1189,768657	1167,764925	1319,075871
2412	1185,200980	1163,893791	1317,478758
2448	1184,434783	1157,109501	1316,551530
2484	1183,317063	1150,498413	1319,192460
2520	1182,723787	1142,415102	1310,753912
2556	1176,290509	1142,068673	1297,003086
2592	1171,586758	1139,992009	1292,485921
2628	1170,917793	1141,074324	1285,987237
2664	1166,326667	1138,895926	1277,450741
2700	1163,039108	1141,267544	1272,657164
2736	1163,833333	1137,997835	1269,121934
2772	1164,007479	1141,727920	1264,556980
2808	1162,762658	1132,169831	1258,868495
2844	1159,093750	1125,929514	1259,506944
2880	1153,255144	1120,809671	1251,492112
2916	1151,474593	1122,025407	1243,287602
2952	1150,888220	1125,400937	1237,823293
2988	1147,984127	1127,633598	1237,476852
3024	1146,597386	1130,577778	1239,460131
3060	1141,775517	1131,563630	1229,669897
3096	1141,355364	1126,340996	1221,578544
3132	1137,642361	1120,450126	1222,291982
3168	1135,023096	1119,266230	1221,021848
3204	1131,452778	1115,785802	1221,419753
3240	1135,363248	1112,279609	1219,690781

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
3276	1134,987621	1107,362319	1213,042271
3312	1130,502091	1107,602748	1203,395460
3348	1125,681738	1105,250296	1199,113475
3384	1127,764327	1101,157018	1192,996199
3420	1131,035301	1102,283565	1187,531250
3456	1127,282073	1102,615407	1180,609966
3492	1124,963152	1103,585884	1179,769558
3528	1128,185466	1100,381313	1178,362795
3564	1125,980000	1100,245556	1179,736667
3600	#N/A	#N/A	#N/A

Ek-3 DB Sorgusu Cevap Süresi Grafiğine Ait İstatistik Verileri

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
0	0	#N/A	#N/A
36	0	#N/A	#N/A
72	0	0,021068	0,019622
108	0	0,023205	0,020251
144	0	0,022406	0,019129
180	0	0,022005	0,018591
216	0	0,021764	0,018252
252	0	0,021604	0,018027
288	0	0,021490	0,017864
324	0	0,021404	0,017742
360	0	0,021337	0,017647
396	0	0,021284	0,017573
432	0	0,021240	0,017518
468	0	0,021203	0,017469
504	0	0,021172	0,017424
540	0	0,021146	0,017385
576	0	0,021123	0,017352

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
612	0	0,021107	0,017326
648	0	0,021089	0,017300
684	0	0,021073	0,017277
720	0	0,021059	0,017258
756	0	0,021046	0,017242
792	0	0,021034	0,017228
828	0	0,021024	0,017214
864	0	0,021014	0,017202
900	0	0,021008	0,017189
936	0	0,020999	0,017177
972	0	0,020992	0,017166
1008	0	0,020985	0,017157
1044	0	0,020978	0,017148
1080	0	0,020972	0,017140
1116	0	0,020966	0,017135
1152	0	0,020961	0,017128
1188	0	0,020956	0,017121
1224	0	0,020951	0,017115
1260	0	0,020947	0,017109
1296	0	0,020943	0,017103
1332	0	0,020939	0,017100
1368	0	0,020935	0,017095
1404	0	0,020932	0,017091
1440	0	0,020929	0,017087
1476	0	0,020925	0,017082
1512	0	0,020922	0,017078
1548	0	0,020920	0,017074
1584	0	0,020917	0,017070
1620	0	0,020914	0,017066
1656	0	0,020912	0,017062
1692	0	0,020909	0,017059
1728	0	0,020907	0,017055
1764	0	0,020905	0,017052
1800	0	0,020903	0,017050
1836	0	0,020901	0,017047
1872	0	0,020899	0,017044

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
1908	0	0,020897	0,017042
1944	0	0,020895	0,017039
1980	0	0,020893	0,017036
2016	0	0,020892	0,017034
2052	0	0,020890	0,017031
2088	0	0,020889	0,017029
2124	0	0,020894	0,017027
2160	0	0,020892	0,017025
2196	0	0,020891	0,017023
2232	0	0,020889	0,017021
2268	0	0,020888	0,017020
2304	0	0,020887	0,017018
2340	0	0,020885	0,017016
2376	0	0,020884	0,017014
2412	0	0,020883	0,017012
2448	0	0,020888	0,017011
2484	0	0,020887	0,017010
2520	0	0,020886	0,017008
2556	0	0,020885	0,017008
2592	0	0,020884	0,017006
2628	0	0,020882	0,017005
2664	0	0,020882	0,017003
2700	0	0,020881	0,017002
2736	0	0,020880	0,017001
2772	0	0,020879	0,017000
2808	0	0,020878	0,016999
2844	0	0,020877	0,016997
2880	0	0,020877	0,016997
2916	0	0,020876	0,016995
2952	0	0,020875	0,016995
2988	0	0,020877	0,016993
3024	0	0,020877	0,016992
3060	0	0,020876	0,016992
3096	0	0,020875	0,016990
3132	0	0,020874	0,016989
3168	0	0,020874	0,016988

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
3204	0	0,020873	0,016987
3240	0	0,020872	0,016986
3276	0	0,020871	0,016985
3312	0	0,020870	0,016985
3348	0	0,020870	0,016984
3384	0	0,020869	0,016983
3420	0	0,020868	0,016983
3456	0	0,020868	0,016981
3492	0	0,020867	0,016980
3528	0	0,020866	0,016980
3564	0	0,020865	0,016979
3600	0	#N/A	#N/A

Ek-4 DB Sorgusu Alınan Trafik Grafiğine Ait İstatistik Verileri

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
0	0	0,000000	0,000000
36	0	0,000000	0,000000
72	0	9,777778	44,000000
108	0	179,666667	704,000000
144	0	237,600000	918,133333
180	0	266,444444	1041,333333
216	0	291,238095	1154,476190
252	0	304,333333	1215,500000
288	0	322,666667	1251,555556
324	0	327,066667	1290,666667
360	0	317,333333	1329,333333
396	0	315,333333	1331,000000
432	0	321,538462	1358,358974
468	0	324,761905	1388,095238
504	0	333,422222	1403,111111

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
540	0	330,000000	1400,666667
576	0	342,509804	1414,039216
612	0	352,814815	1436,518519
648	0	352,771930	1428,818713
684	0	354,933333	1446,866667
720	0	356,190476	1457,587302
756	0	354,666667	1473,333333
792	0	358,376812	1478,782609
828	0	367,277778	1472,777778
864	0	366,080000	1476,053333
900	0	367,230769	1480,769231
936	0	368,839506	1478,074074
972	0	366,666667	1485,523810
1008	0	368,183908	1493,471264
1044	0	366,666667	1496,977778
1080	0	367,612903	1508,774194
1116	0	369,416667	1513,875000
1152	0	366,222222	1522,666667
1188	0	368,823529	1529,647059
1224	0	369,600000	1540,000000
1260	0	367,888889	1547,333333
1296	0	366,270270	1555,063063
1332	0	367,438596	1554,280702
1368	0	368,923077	1550,905983
1404	0	367,400000	1553,200000
1440	0	366,666667	1558,959350
1476	0	366,666667	1562,698413
1512	0	368,372093	1559,782946
1548	0	368,333333	1564,000000
1584	0	366,004938	1562,814815
1620	0	366,028986	1570,608696
1656	0	366,978723	1571,205674
1692	0	369,722222	1571,166667
1728	0	370,258503	1582,503401
1764	0	371,653333	1584,880000
1800	0	369,542484	1588,601307

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
1836	0	368,923077	1591,615385
1872	0	369,433962	1596,176101
1908	0	368,567901	1598,395062
1944	0	369,333333	1597,066667
1980	0	371,119048	1599,714286
2016	0	373,099415	1604,842105
2052	0	374,000000	1599,931034
2088	0	373,627119	1596,926554
2124	0	374,000000	1597,444444
2160	0	373,158470	1598,185792
2196	0	374,946237	1602,215054
2232	0	375,047619	1601,925926
2268	0	375,604167	1603,937500
2304	0	377,046154	1604,307692
2340	0	377,111111	1606,000000
2376	0	378,049751	1603,701493
2412	0	378,529412	1607,078431
2448	0	378,782609	1606,956522
2484	0	379,028571	1610,609524
2520	0	377,615023	1611,061033
2556	0	377,259259	1611,092593
2592	0	376,913242	1611,926941
2628	0	376,774775	1614,720721
2664	0	378,400000	1613,920000
2700	0	377,473684	1615,070175
2736	0	376,952381	1618,857143
2772	0	378,888889	1618,786325
2808	0	379,105485	1618,717300
2844	0	378,583333	1622,500000
2880	0	378,255144	1624,016461
2916	0	377,398374	1625,317073
2952	0	375,678715	1627,116466
2988	0	375,047619	1629,396825
3024	0	373,913725	1631,450980
3060	0	373,317829	1632,263566
3096	0	372,567050	1630,191571

Zaman (saniye)	saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
3132	0	373,333333	1631,000000
3168	0	374,741573	1632,609238
3204	0	374,325926	1634,518519
3240	0	375,047619	1636,542125
3276	0	374,478261	1637,724638
3312	0	376,759857	1639,670251
3348	0	376,652482	1640,014184
3384	0	375,775439	1638,189474
3420	0	376,597222	1636,861111
3456	0	376,646048	1638,584192
3492	0	375,945578	1637,877551
3528	0	376,296296	1637,925926
3564	0	376,640000	1637,826667
3600	#N/A	#N/A	#N/A

Ek-5 Eposta İndirme Yanıt Süresi Grafiğine Ait İstatistik Verileri

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
0	#N/A	#N/A	#N/A
36	#N/A	#N/A	#N/A
72	0,065504	0,069619	0,063432
108	0,073194	0,080835	0,069139
144	0,065442	0,080835	0,061464
180	0,061567	0,071829	0,057627
216	0,059241	0,071829	0,055327
252	0,057691	0,067099	0,053792
288	0,057691	0,067099	0,052696
324	0,057691	0,064350	0,051875
360	0,056576	0,062494	0,051236
396	0,055747	0,061251	0,050724
432	0,055747	0,060300	0,050724

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
468	0,055104	0,059519	0,050306
504	0,055104	0,058902	0,049957
540	0,054588	0,058438	0,049740
576	0,054588	0,058052	0,049481
612	0,054166	0,057726	0,049257
648	0,053814	0,057414	0,049257
684	0,053516	0,057143	0,049082
720	0,053516	0,056948	0,048908
756	0,053260	0,056763	0,048763
792	0,053040	0,056598	0,048623
828	0,052846	0,056420	0,048498
864	0,052671	0,056259	0,048498
900	0,052519	0,056175	0,048386
936	0,052384	0,056068	0,048283
972	0,052263	0,055950	0,048189
1008	0,052153	0,055950	0,048102
1044	0,052052	0,055860	0,048023
1080	0,051960	0,055754	0,047950
1116	0,051877	0,055679	0,047883
1152	0,051877	0,055610	0,047820
1188	0,051799	0,055546	0,047762
1224	0,051728	0,055471	0,047748
1260	0,051662	0,055415	0,047696
1296	0,051600	0,055415	0,047647
1332	0,051543	0,055349	0,047630
1368	0,051611	0,055301	0,047630
1404	0,051557	0,055256	0,047586
1440	0,051506	0,055204	0,047544
1476	0,051459	0,055164	0,047506
1512	0,051415	0,055164	0,047468
1548	0,051373	0,055126	0,047432
1584	0,051333	0,055091	0,047432
1620	0,051296	0,055056	0,047399
1656	0,051260	0,055017	0,047367
1692	0,051226	0,054975	0,047336
1728	0,051211	0,054946	0,047307

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
1764	0,051180	0,054919	0,047279
1800	0,051150	0,054919	0,047253
1836	0,051122	0,054872	0,047249
1872	0,051122	0,054848	0,047225
1908	0,051095	0,054819	0,047201
1944	0,051095	0,054796	0,047178
1980	0,051070	0,054775	0,047178
2016	0,051045	0,054755	0,047157
2052	0,051022	0,054736	0,047140
2088	0,050999	0,054736	0,047120
2124	0,050999	0,054711	0,047101
2160	0,050978	0,054711	0,047157
2196	0,050957	0,054676	0,047157
2232	0,050937	0,054652	0,047137
2268	0,050918	0,054636	0,047137
2304	0,050900	0,054620	0,047119
2340	0,050882	0,054605	0,047101
2376	0,050865	0,054575	0,047094
2412	0,050849	0,054561	0,047077
2448	0,050833	0,054549	0,047061
2484	0,050818	0,054536	0,047045
2520	0,050803	0,054524	0,047031
2556	0,050788	0,054507	0,047016
2592	0,050775	0,054491	0,047025
2628	0,050765	0,054470	0,047010
2664	0,050757	0,054459	0,046997
2700	0,050744	0,054449	0,046983
2736	0,050731	0,054439	0,046971
2772	0,050719	0,054426	0,046959
2808	0,050708	0,054410	0,046946
2844	0,050696	0,054388	0,046954
2880	0,050685	0,054391	0,046942
2916	0,050675	0,054383	0,046931
2952	0,050665	0,054371	0,046920
2988	0,050655	0,054351	0,046920
3024	0,050645	0,054331	0,046909

Zaman (saniye)	yanıt süresi(saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
3060	0,050635	0,054331	0,046903
3096	0,050626	0,054318	0,046892
3132	0,050617	0,054312	0,046884
3168	0,050608	0,054299	0,046874
3204	0,050600	0,054285	0,046865
3240	0,050592	0,054285	0,046858
3276	0,050583	0,054279	0,046849
3312	0,050576	0,054267	0,046841
3348	0,050568	0,054271	0,046833
3384	0,050568	0,054265	0,046825
3420	0,050560	0,054260	0,046817
3456	0,050553	0,054260	0,046809
3492	0,050546	0,054260	0,046809
3528	0,050539	0,054249	0,046801
3564	0,050532	0,054274	0,046811
3600	#N/A	#N/A	#N/A

Ek-6 Eposta Alınan Trafik Grafiğine Ait İstatistik Verileri

Zaman (saniye)	Saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
0	0,000000	0,000000	0,000000
36	0,000000	0,000000	0,000000
72	449,185185	449,185185	716,037037
108	4232,166667	4221,638889	4916,472222
144	3411,000000	3377,311111	3950,022222
180	2870,574074	2821,444444	3312,740741
216	2496,587302	2424,396825	2869,571429
252	2210,833333	2137,138889	2516,138889
288	1974,543210	1913,716049	2259,962963
324	1798,144444	1734,977778	2059,233333
360	1646,161616	1592,565657	1891,171717

Zaman (saniye)	Saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
396	1523,018519	1473,888889	1754,629630
432	1412,341880	1376,709402	1626,136752
468	1323,492063	1296,420635	1534,047619
504	1238,066667	1224,029630	1437,392593
540	1176,479167	1150,159722	1355,451389
576	1112,228758	1089,934641	1283,150327
612	1062,135802	1036,401235	1223,561728
648	1015,099415	988,502924	1163,596491
684	970,661111	945,394444	1115,944444
720	932,460317	906,391534	1068,820106
756	899,646465	869,020202	1035,550505
792	871,516908	840,391304	994,188406
828	840,467593	812,393519	958,027778
864	815,271111	784,951111	921,391111
900	790,393162	766,098291	889,192308
936	767,358025	740,843621	862,497942
972	742,960317	718,896825	842,222222
1008	723,149425	699,915709	818,988506
1044	704,659259	680,796296	797,303704
1080	691,437276	668,344086	777,017921
1116	672,461806	651,406250	760,631944
1152	654,636364	634,218855	749,067340
1188	637,859477	618,042484	734,467320
1224	624,447619	602,790476	718,295238
1260	615,290123	589,555556	703,021605
1296	605,489489	574,759760	689,711712
1332	598,421053	564,067251	680,426901
1368	586,316239	558,242165	665,139601
1404	572,711111	546,391667	657,986111
1440	561,823848	536,146341	652,208672
1476	554,462963	532,404762	642,695767
1512	545,485788	521,981912	634,604651
1548	536,916667	513,946970	624,010101
1584	530,600000	507,204938	612,950617
1620	523,642512	499,840580	606,033816
1656	516,981087	494,581560	597,619385

Zaman (saniye)	Saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
1692	513,229167	487,787037	588,678241
1728	507,911565	481,269841	578,383220
1764	500,280000	472,486667	572,711111
1800	494,599129	463,222222	564,784314
1836	488,326923	455,933761	558,782051
1872	479,907757	448,920335	550,622642
1908	472,580247	443,726337	541,985597
1944	467,816162	437,189899	534,428283
1980	460,214286	432,390873	527,892857
2016	455,834308	427,760234	522,325536
2052	452,331418	425,467433	520,580460
2088	446,092279	418,969868	515,325800
2124	443,570370	414,794444	509,544444
2160	441,821494	409,375228	509,475410
2196	436,732975	404,810036	502,616487
2232	430,469136	401,726631	499,317460
2268	426,375000	398,739583	492,173611
2304	421,111111	394,548718	487,193162
2340	416,006734	391,122896	481,725589
2376	413,568823	387,799337	478,935323
2412	408,725490	383,954248	473,130719
2448	404,632850	379,610306	469,325282
2484	401,860317	374,788889	466,230159
2520	401,538341	371,289515	462,035994
2556	396,546296	369,057099	458,543210
2592	392,267884	366,885845	456,299848
2628	388,105105	365,342342	451,840841
2664	387,422222	363,840000	447,500741
2700	384,540936	360,714912	443,828947
2736	382,828283	358,217893	440,252525
2772	379,000000	355,784900	436,767806
2808	377,400844	352,880450	433,371308
2844	375,315278	350,575000	432,165278
2880	372,241427	349,886145	428,909465
2916	370,783198	346,646341	427,273713
2952	368,345382	346,528782	425,677376

Zaman (saniye)	Saniye başına alınan bayt miktarı(bayt/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
2988	366,466931	346,414021	423,116402
3024	363,641830	343,824837	421,111111
3060	363,330749	340,316537	420,131783
3096	361,090677	339,793103	418,206897
3132	357,944444	337,367424	415,847222
3168	355,815231	335,942572	412,121099
3204	352,797531	333,613580	408,477778
3240	350,308913	330,873016	408,153846
3276	349,247585	329,565217	405,090580
3312	346,397849	329,191159	401,187575
3348	344,952719	327,481087	398,263593
3384	342,208187	325,363743	396,287719
3420	340,836806	322,851852	394,791667
3456	339,059565	320,391753	392,892325
3492	336,459184	317,981859	390,602041
3528	333,485971	316,046016	389,208754
3564	333,098889	314,148889	387,843333
3600	#N/A	#N/A	#N/A

Ek-7 internet-ra bağlantı kullanımı (DS1-E1) Grafiklerine Ait İstatistik Verileri

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
0	0,003425	0,004275	0,006290	0,002159	0,002799	0,002159
36	0,003145	0,003713	0,003145	0,002159	0,002588	0,002159
72	0,166460	0,181386	0,211812	0,102677	0,113925	0,130816
108	1,860913	2,048017	2,183096	1,150464	1,197027	1,398882
144	1,524275	1,757127	1,871690	0,924792	1,018336	1,221825
180	1,302341	1,558422	1,700876	0,783330	0,900316	1,101729
216	1,134906	1,410932	1,549254	0,692939	0,823259	1,017645
252	1,033950	1,311505	1,446395	0,629144	0,758606	0,951983
288	0,948701	1,224763	1,354766	0,583233	0,712395	0,889152

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
324	0,888896	1,146095	1,289551	0,533792	0,666732	0,850922
360	0,822384	1,067406	1,239373	0,500489	0,638627	0,810681
396	0,782657	1,025558	1,216501	0,465979	0,609553	0,778621
432	0,729569	0,979598	1,173981	0,447322	0,590893	0,761305
468	0,697586	0,937966	1,166302	0,428420	0,577649	0,739812
504	0,666530	0,915078	1,136530	0,412991	0,565737	0,730999
540	0,642886	0,888947	1,107449	0,393054	0,552124	0,724075
576	0,606780	0,867717	1,079559	0,375237	0,540601	0,712186
612	0,586669	0,849065	1,070797	0,360992	0,535299	0,699445
648	0,565529	0,821050	1,053587	0,348910	0,521049	0,691166
684	0,545435	0,809412	1,043413	0,335813	0,510979	0,686812
720	0,530641	0,799332	1,032545	0,326282	0,501790	0,674088
756	0,516419	0,782064	1,022343	0,320282	0,493205	0,665164
792	0,502532	0,767893	1,009644	0,311752	0,486264	0,654880
828	0,496440	0,763584	0,991954	0,307230	0,482564	0,651232
864	0,487283	0,751935	0,984995	0,301714	0,476895	0,644904
900	0,475272	0,744458	0,972378	0,296512	0,472662	0,642819
936	0,464361	0,739432	0,963746	0,289798	0,468157	0,637603
972	0,457352	0,731641	0,955769	0,282246	0,463120	0,628547
1008	0,445554	0,729195	0,949875	0,275402	0,455098	0,623386
1044	0,436914	0,718546	0,943268	0,269317	0,453371	0,619070
1080	0,434526	0,708333	0,943471	0,265409	0,450633	0,616780
1116	0,424589	0,704169	0,935902	0,260769	0,448341	0,609950
1152	0,416337	0,693419	0,930501	0,256456	0,445063	0,607618
1188	0,407667	0,690479	0,927574	0,251163	0,441291	0,602983
1224	0,404453	0,688323	0,926475	0,247003	0,437711	0,601966
1260	0,403023	0,683880	0,926355	0,244183	0,434784	0,599747
1296	0,406490	0,679419	0,922022	0,240459	0,433316	0,597184
1332	0,405003	0,672545	0,920110	0,238592	0,429519	0,596274
1368	0,400618	0,667422	0,916940	0,236088	0,426366	0,593875
1404	0,395545	0,664611	0,913611	0,234683	0,425298	0,589454
1440	0,387771	0,661275	0,911779	0,232617	0,422900	0,585634
1476	0,384382	0,661202	0,910955	0,230360	0,420246	0,583795
1512	0,380406	0,656459	0,907184	0,228875	0,419792	0,580461
1548	0,380668	0,650264	0,903950	0,227301	0,420507	0,578916
1584	0,380223	0,649459	0,900956	0,224536	0,417318	0,577122

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
1620	0,376118	0,646055	0,899923	0,223261	0,416430	0,576038
1656	0,369523	0,644490	0,899870	0,221177	0,413276	0,576732
1692	0,369784	0,644960	0,895300	0,219687	0,410618	0,576774
1728	0,366871	0,642848	0,898951	0,215805	0,412060	0,577337
1764	0,365051	0,639041	0,896306	0,215059	0,409592	0,574439
1800	0,363321	0,633698	0,895199	0,215266	0,408368	0,572735
1836	0,358769	0,629317	0,891768	0,212250	0,405706	0,572722
1872	0,358268	0,627485	0,889240	0,209849	0,405176	0,572297
1908	0,354267	0,622279	0,884782	0,208365	0,404369	0,569317
1944	0,353466	0,618106	0,882800	0,206624	0,402519	0,569065
1980	0,349313	0,616070	0,883128	0,205608	0,401169	0,568972
2016	0,347028	0,615390	0,881996	0,205439	0,399928	0,566938
2052	0,346503	0,615572	0,878709	0,202299	0,398543	0,564623
2088	0,344416	0,614305	0,876129	0,201904	0,398621	0,563871
2124	0,343491	0,612344	0,876604	0,200754	0,397424	0,561357
2160	0,341544	0,612383	0,876924	0,199211	0,395704	0,560864
2196	0,340280	0,611605	0,877854	0,196312	0,395398	0,560261
2232	0,338514	0,610840	0,879305	0,194800	0,395265	0,559396
2268	0,336669	0,609861	0,877136	0,195155	0,393212	0,559303
2304	0,335507	0,608847	0,874265	0,193603	0,392025	0,557599
2340	0,331684	0,609434	0,873944	0,191553	0,391021	0,556938
2376	0,329664	0,609558	0,872565	0,190660	0,390368	0,555844
2412	0,327158	0,608323	0,871371	0,190387	0,388773	0,555058
2448	0,324779	0,607140	0,868858	0,190296	0,388203	0,554124
2484	0,323268	0,604590	0,867753	0,189208	0,387878	0,552921
2520	0,322874	0,602407	0,864810	0,187800	0,386838	0,551418
2556	0,320513	0,601720	0,861004	0,186759	0,387076	0,552410
2592	0,320381	0,601806	0,860006	0,185058	0,387383	0,552200
2628	0,320050	0,601560	0,857718	0,183655	0,387931	0,551041
2664	0,319131	0,602669	0,855433	0,182720	0,385892	0,549618
2700	0,317086	0,601235	0,853764	0,182019	0,384615	0,547308
2736	0,316360	0,599063	0,854355	0,181053	0,386522	0,547014
2772	0,315386	0,599637	0,853131	0,180035	0,387330	0,546939
2808	0,315177	0,598647	0,850720	0,179311	0,386338	0,546231
2844	0,314606	0,597107	0,851040	0,179558	0,385802	0,546248
2880	0,313480	0,595686	0,850437	0,178834	0,384213	0,544878

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
2916	0,312407	0,592895	0,848771	0,177788	0,383343	0,543400
2952	0,310348	0,593095	0,849209	0,177914	0,383177	0,541797
2988	0,309373	0,592969	0,848772	0,176063	0,381701	0,543149
3024	0,307423	0,593028	0,848888	0,175350	0,381433	0,543297
3060	0,306233	0,592384	0,846100	0,174748	0,381280	0,544173
3096	0,306467	0,591010	0,843602	0,174601	0,380683	0,544923
3132	0,303501	0,590260	0,843958	0,174939	0,380572	0,543535
3168	0,301986	0,591357	0,842389	0,175247	0,379868	0,543800
3204	0,300211	0,590714	0,841996	0,174692	0,379715	0,543005
3240	0,300211	0,589197	0,843721	0,174110	0,378917	0,543088
3276	0,299972	0,587768	0,842010	0,173199	0,377316	0,543351
3312	0,298736	0,589022	0,839379	0,172212	0,377514	0,542389
3348	0,296897	0,587702	0,837710	0,172433	0,377463	0,541874
3384	0,296886	0,585675	0,835331	0,172464	0,376878	0,542542
3420	0,297818	0,584704	0,835276	0,172086	0,376551	0,542991
3456	0,297557	0,584212	0,834207	0,172450	0,376697	0,543535
3492	0,296916	0,584702	0,833431	0,172336	0,375535	0,544208
3528	0,297394	0,583192	0,831672	0,171276	0,375165	0,544130
3564	0,297379	0,582501	0,831037	0,170738	0,373845	0,542396
3600	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A

Ek-8 internet-rb bağlantı kullanımı (DS1-E1) Grafiklerine Ait İstatistik Verileri

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall _no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
0	0,003425	0,003713	0,003425	0,002159	0,002799	0,002159
36	0,003145	0,003433	0,003145	0,002159	0,002588	0,002159
72	0,204040	0,165731	0,330604	0,125760	0,102384	0,210529
108	1,728184	1,842581	2,253710	1,027702	1,077409	1,410273
144	1,452496	1,495409	1,993952	0,843312	0,885352	1,244080
180	1,234132	1,266211	1,792753	0,714471	0,762862	1,124929
216	1,069420	1,107073	1,694738	0,633974	0,671041	1,048600

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall _no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
252	0,961791	0,992773	1,582290	0,568392	0,604681	1,008373
288	0,877930	0,891149	1,503742	0,519381	0,542673	0,955898
324	0,810841	0,812352	1,449275	0,469678	0,507292	0,920856
360	0,755618	0,769222	1,392953	0,438103	0,478956	0,891078
396	0,702612	0,720706	1,341679	0,409910	0,450170	0,863794
432	0,660272	0,676596	1,302319	0,385983	0,423705	0,841232
468	0,623630	0,642748	1,264446	0,371191	0,397163	0,806473
504	0,594053	0,612943	1,246365	0,354280	0,381628	0,792915
540	0,575687	0,579476	1,205607	0,340674	0,365157	0,775262
576	0,552490	0,558610	1,184596	0,328256	0,358053	0,758130
612	0,537096	0,542751	1,171470	0,314995	0,342063	0,743691
648	0,516651	0,525750	1,139924	0,300547	0,328916	0,729102
684	0,493023	0,510915	1,133576	0,289530	0,320065	0,723572
720	0,478116	0,492342	1,124270	0,279428	0,312653	0,719039
756	0,461135	0,481863	1,118846	0,274823	0,301466	0,710517
792	0,452442	0,474115	1,102412	0,266592	0,295253	0,700888
828	0,442661	0,461800	1,093493	0,258738	0,287280	0,692103
864	0,435481	0,445092	1,081454	0,254160	0,282336	0,689553
900	0,425680	0,441601	1,067596	0,246849	0,276240	0,683118
936	0,422010	0,435362	1,053333	0,241475	0,270546	0,676415
972	0,409527	0,426313	1,049617	0,236263	0,263585	0,670267
1008	0,405540	0,414238	1,047359	0,234444	0,257363	0,664335
1044	0,403353	0,404227	1,041834	0,230995	0,253957	0,657453
1080	0,396817	0,397616	1,038803	0,228904	0,248429	0,654332
1116	0,390219	0,388593	1,036798	0,223695	0,246971	0,651222
1152	0,385873	0,378974	1,031133	0,221418	0,244327	0,648499
1188	0,380318	0,369105	1,025240	0,217921	0,239994	0,646691
1224	0,374802	0,365266	1,022045	0,213526	0,236846	0,642109
1260	0,374391	0,361307	1,015337	0,211699	0,235565	0,640575
1296	0,368750	0,359862	1,010139	0,210040	0,232037	0,639123
1332	0,367492	0,356793	1,004594	0,206922	0,230377	0,638057
1368	0,365184	0,354595	0,997288	0,204342	0,229120	0,634008
1404	0,360888	0,351332	0,997485	0,200302	0,228065	0,632731
1440	0,354864	0,347674	0,992241	0,198692	0,225670	0,628651
1476	0,352108	0,346633	0,990153	0,198180	0,223464	0,625995
1512	0,346747	0,342789	0,989153	0,196460	0,220479	0,621781

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall _no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
1548	0,340840	0,339105	0,982974	0,192492	0,219386	0,620679
1584	0,336398	0,337291	0,974794	0,190273	0,217801	0,617376
1620	0,338057	0,333487	0,977313	0,190395	0,216644	0,618551
1656	0,333800	0,333326	0,975322	0,187229	0,215206	0,619695
1692	0,334819	0,328928	0,972518	0,186091	0,214163	0,616774
1728	0,333459	0,326121	0,977303	0,184674	0,214965	0,614394
1764	0,330917	0,325048	0,976741	0,182734	0,211484	0,611227
1800	0,330497	0,321700	0,969151	0,182838	0,209707	0,611263
1836	0,327778	0,318262	0,967036	0,182543	0,208844	0,610325
1872	0,325228	0,316673	0,965849	0,181821	0,206715	0,609554
1908	0,322792	0,317370	0,962795	0,180555	0,206829	0,607579
1944	0,321459	0,316384	0,959602	0,179898	0,206778	0,605376
1980	0,317090	0,315929	0,956848	0,178947	0,205885	0,605735
2016	0,314375	0,312308	0,955407	0,177929	0,203994	0,604407
2052	0,312438	0,311720	0,953345	0,176628	0,202653	0,601904
2088	0,310374	0,309691	0,949888	0,175560	0,201249	0,599745
2124	0,309965	0,307056	0,948833	0,175421	0,201330	0,599958
2160	0,309352	0,306991	0,946143	0,174162	0,200128	0,598536
2196	0,308768	0,304195	0,943850	0,171740	0,197865	0,598336
2232	0,307005	0,301333	0,946013	0,170380	0,197437	0,596820
2268	0,304567	0,300371	0,946197	0,169010	0,197244	0,596850
2304	0,301653	0,302567	0,949601	0,168670	0,194831	0,594099
2340	0,298925	0,300579	0,946977	0,167708	0,196607	0,592300
2376	0,297534	0,299532	0,945426	0,167116	0,195403	0,590641
2412	0,296370	0,298014	0,945885	0,165783	0,194177	0,589138
2448	0,296372	0,294891	0,947651	0,165715	0,192842	0,590267
2484	0,295677	0,292853	0,951076	0,163596	0,192533	0,588946
2520	0,295492	0,289900	0,948984	0,162817	0,191220	0,586253
2556	0,293077	0,289046	0,946022	0,161571	0,189574	0,585600
2592	0,289442	0,287017	0,945235	0,160590	0,189299	0,585584
2628	0,287665	0,286686	0,944985	0,159377	0,187776	0,583531
2664	0,286305	0,285464	0,941220	0,159019	0,186513	0,582548
2700	0,285196	0,285882	0,940599	0,157494	0,187113	0,580973
2736	0,285326	0,285930	0,939937	0,156869	0,186717	0,580753
2772	0,284604	0,286742	0,938872	0,155902	0,186385	0,582158
2808	0,284063	0,283146	0,937363	0,154665	0,185308	0,581801

Zaman (saniye)	DS1 (kullanım oranı)			E1 (kullanım oranı)		
	firewall_ no_vpn	firewall_ vpn	no_firewall _no_vpn	firewall_ no_vpn	firewall_ vpn	no_firewall_ no_vpn
2844	0,282620	0,280567	0,938731	0,154241	0,184325	0,581241
2880	0,280422	0,279432	0,935830	0,153300	0,183660	0,580109
2916	0,280134	0,280761	0,934265	0,153176	0,183079	0,579619
2952	0,281156	0,280883	0,932408	0,152052	0,182994	0,578769
2988	0,279757	0,281721	0,933193	0,151740	0,182195	0,578667
3024	0,279754	0,280960	0,935308	0,151962	0,182167	0,579508
3060	0,277958	0,280256	0,934288	0,151734	0,182436	0,578794
3096	0,276839	0,279537	0,931630	0,151164	0,181655	0,579020
3132	0,276797	0,277621	0,930830	0,150813	0,181274	0,580317
3168	0,275909	0,276580	0,931004	0,149740	0,181431	0,580114
3204	0,275025	0,274368	0,931106	0,150455	0,179832	0,580096
3240	0,275683	0,274167	0,929538	0,149566	0,179525	0,580033
3276	0,275525	0,272548	0,928201	0,149356	0,178886	0,578617
3312	0,273815	0,272387	0,926295	0,148600	0,178150	0,578310
3348	0,273173	0,272245	0,925157	0,148518	0,177562	0,579472
3384	0,273000	0,270974	0,922951	0,149098	0,177556	0,580321
3420	0,272862	0,271665	0,919716	0,149443	0,177574	0,579004
3456	0,270854	0,271408	0,918496	0,148370	0,177802	0,577635
3492	0,269311	0,270097	0,916946	0,148199	0,176991	0,576362
3528	0,268580	0,269633	0,917833	0,146937	0,177989	0,575785
3564	0,267638	0,269925	0,918322	0,146313	0,177840	0,575818
3600	#N/A	#N/A	#N/A	#N/A	#N/A	#N/A

Ek-9 Sunucu Yük Performansı Grafiğine Ait İstatistik Verileri

Zaman (saniye)	Saniyede cevaplanan istek sayısı(istek/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
0	0,000000	0,000000	0,000000
36	0,000000	0,000000	0,000000
72	0,842593	0,666667	1,000000
108	7,875000	8,291667	8,625000
144	6,600000	6,833333	7,166667

Zaman (saniye)	Saniyede cevaplanan istek sayısı(istek/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
180	5,694444	5,944444	6,305556
216	4,952381	5,285714	5,642857
252	4,562500	4,854167	5,125000
288	4,259259	4,388889	4,703704
324	4,016667	4,033333	4,400000
360	3,787879	3,818182	4,136364
396	3,625000	3,652778	4,027778
432	3,410256	3,435897	3,807692
468	3,273810	3,273810	3,690476
504	3,166667	3,155556	3,600000
540	3,114583	3,041667	3,437500
576	2,970588	2,941176	3,303922
612	2,925926	2,861111	3,240741
648	2,833333	2,763158	3,140351
684	2,733333	2,725000	3,108333
720	2,666667	2,674603	3,071429
756	2,590909	2,628788	3,015152
792	2,550725	2,573671	2,942029
828	2,541667	2,534722	2,902778
864	2,520000	2,473333	2,866667
900	2,467949	2,455128	2,788462
936	2,444444	2,450617	2,740741
972	2,404762	2,428571	2,708333
1008	2,373563	2,390805	2,689655
1044	2,361111	2,344444	2,661111
1080	2,344086	2,290323	2,655914
1116	2,307292	2,260417	2,625000
1152	2,282828	2,212121	2,580808
1188	2,254902	2,181373	2,544118
1224	2,242857	2,180952	2,528571
1260	2,254630	2,171296	2,500000
1296	2,261261	2,175676	2,463964
1332	2,258772	2,154240	2,447368
1368	2,256410	2,128205	2,431624
1404	2,241667	2,129167	2,425000
1440	2,203252	2,121951	2,390244

Zaman (saniye)	Saniyede cevaplanan istek sayısı(istek/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
1476	2,186508	2,126984	2,384921
1512	2,162791	2,104651	2,379845
1548	2,159091	2,075758	2,348485
1584	2,148148	2,081481	2,318519
1620	2,152174	2,061594	2,315217
1656	2,120567	2,063830	2,319149
1692	2,131944	2,052083	2,302083
1728	2,125850	2,040816	2,326531
1764	2,120000	2,033333	2,316667
1800	2,120915	2,019608	2,284314
1836	2,102564	2,000000	2,262821
1872	2,103774	1,996855	2,248428
1908	2,089506	1,993827	2,225309
1944	2,084848	1,981818	2,218182
1980	2,062500	1,973214	2,208333
2016	2,046784	1,956140	2,192982
2052	2,043103	1,951149	2,186782
2088	2,036723	1,949153	2,177966
2124	2,030556	1,938889	2,180556
2160	2,021858	1,948087	2,166667
2196	2,024194	1,935484	2,161290
2232	2,021164	1,928571	2,182540
2268	2,010417	1,924479	2,177083
2304	2,002564	1,933333	2,184615
2340	1,984848	1,931818	2,176768
2376	1,975124	1,930348	2,176617
2412	1,968137	1,924020	2,174020
2448	1,966184	1,913043	2,172705
2484	1,964286	1,902381	2,178571
2520	1,962441	1,889671	2,164319
2556	1,951389	1,888889	2,141204
2592	1,942922	1,885845	2,134703
2628	1,941441	1,887387	2,123874
2664	1,933333	1,884444	2,108889
2700	1,927632	1,888158	2,100877
2736	1,928571	1,883117	2,095238

Zaman (saniye)	Saniyede cevaplanan istek sayısı(istek/saniye)		
	firewall_no_vpn	firewall_vpn	no_firewall_no_vpn
2772	1,929487	1,888889	2,087607
2808	1,928270	1,873418	2,078059
2844	1,922917	1,862500	2,079167
2880	1,913580	1,853909	2,065844
2916	1,910569	1,855691	2,052846
2952	1,909639	1,861446	2,044177
2988	1,904762	1,865079	2,043651
3024	1,901961	1,870588	2,047059
3060	1,893411	1,872093	2,031008
3096	1,892720	1,863985	2,017241
3132	1,886364	1,854167	2,018939
3168	1,882022	1,852060	2,016854
3204	1,875926	1,846296	2,016667
3240	1,882784	1,840659	2,014652
3276	1,882246	1,833333	2,003623
3312	1,874552	1,833333	1,987455
3348	1,867021	1,829787	1,980496
3384	1,870175	1,822807	1,970175
3420	1,875000	1,824653	1,961806
3456	1,869416	1,824742	1,950172
3492	1,865646	1,826531	1,948980
3528	1,870370	1,821549	1,946128
3564	1,866667	1,821667	1,948333
3600	#N/A	#N/A	#N/A

ÖZGEÇMİŞ

Adı Soyadı : Serkan ÇAM

Telefon : 0505 932 9004

E-Posta : serkancam22@gmail.com

15.10.1982 yılında Edirne'de doğdu. İlk ve orta öğrenimini Edirne'de tamamladı. 2000 yılında Tekirdağ Teknik Lisesi Elektronik Bölümünden mezun oldu. 2005 yılında Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Öğretmenliği Bölümünü bitirdi. Hâlen Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalında tez çalışmasına devam etmektedir.

2006 yılında Düzce/Kaynaşlı Sarıçökek Köyü İlköğretim Okuluna Bilişim Teknolojileri Öğretmeni olarak atandı. Sırasıyla 2006-2008 yılları arasında Düzce/Kaynaşlı Sarıçökek Köyü İlköğretim Okulu, 2008-2010 yılları arasında İstanbul/Silivri Namık Kemal İlköğretim Okulu, 2010-2016 yılları arasında Silivri Mesleki ve Teknik Anadolu Lisesi ve 2016-2017 yılları arasında Edirne/Süloğlu Cumhuriyet Orta Okulunda Bilişim Teknolojileri Öğretmeni olarak görev yaptı. 2017 yılından beri Edirne Şehit Nefize ÇETİN ÖZSOY Bilim ve Sanat Merkezinde Bilişim Teknolojileri Öğretmeni olarak görev yapmaktadır.

Evli ve iki çocuk babasıdır.