

SQUID PROXY İLE GERÇEK ZAMANLI WEB TRAFİK KONTROLÜ

Erhan YELİ
Fırat Üniversitesi
Bilgisayar Müh. Bölümü
erhanyeli@hotmail.com

Gürkan KARABATAK **Yrd.Doç.Dr Hasan H.BALIK**
Fırat Üniversitesi
Enformatik Bölümü
gkarabatak@firat.edu.tr balik@firat.edu.tr

ÖZET

Üniversite içerisindeki ağdan internete giren kullanıcıların web trafiğinin gerçek zamanlı olarak kontrol edilip, izlenmesi. İzleme işlemi trace.firat.edu.tr adresindeki web arayüzü ile dinamik olarak yapılabilmektedir. İzleme işlemi site admini tarafından açılan kullanıcılar tarafından yapılabilmektedir. Her kullanıcıya belirli sınırlamalar verilir. Yani her kullanıcı istediği her şeyi izleyemez. Adminin verdiği haklar çerçevesinde izleme işlemini yapabilir.

Ayrıca üniversite içerisindeki öğrenci laboratuvarlarının daha etkin ve faydalı olarak kullanılması. Bu işlem laboratuvar sorumlularına açılan kullanıcılar ile laboratuvarların gerçek zamanlı izlenmesiyle sağlanır.

Üniversite laboratuvarları genel kullanımda olduğu için internet üzerinden yapılan suçlara açık yerlerdir. Gerçek zamanlı izleme sistemi caydırıcı bir önlem olabilir bu bu suçların önüne geçilebilir.

1. GİRİŞ

Üniversite içerisindeki ağdan internete giren kullanıcıların web trafiğinin gerçek zamanlı olarak kontrol edilip izleme işlemi <http://trace.firat.edu.tr> adresindeki web arayüzü ile dinamik olarak hızlı ve güvenli bir şekilde yapılabilmektedir. Site kullanıcıları internete bağlı herhangi bir bilgisayardan kendilerine tanınan haklar çerçevesinde gerçek zamanlı web trafik kontrolü işlemini yapabilirler.

Gerçek zamanlı web trafik kontrolünde Linux Redhat 9.0 üzerinde çalışan Squid Proxy Server önemli bir iş yapmaktadır. Proje Squid Proxy ile entegre çalışmaktadır. Squid Proxy'den alınan verilerin anında işlenmekte ve trace.firat.edu.tr adresinde site kullanıcılarına anında gösterilmektedir.

Projede web programlama dili olarak PHP; Veritabanı olarak MySQL kullanılmıştır. PHP kullanılmasının nedeni Linux altında çok verimli, performanslı ve hızlı olmasıdır ayrıca veritabanıyla

çok uyumlu çalışabilmesidir. Veritabanının MySQL seçilmesinin nedeni PHP ile en uyumlu çalışabilen veritabanı olması, bu çok karmaşık olmayan verilerin tasnif edilmesinde en performanlı veritabanı olmasıdır. Hız ve performans için MySQL seçilmiştir.

Squid Proxy Server'dan alınan veriler PHP ile parse edilerek MySQL' e aktarılır. Sonra PHP ile MySQL sorgulanır ve sonuçlar web adresine aktarılır. Bu işlemlerin hepsi gerçek zamanlı olarak yapılmaktadır.

2. YÖNETİCİ ARABİRİMİ

Site yöneticisi kullanıcıları siteye ekler ve kullanıcı haklarını düzenler. Aşağıdaki işlemleri admin modülü ile yapabilir.

- Gerçek zamanlı web trafik kontrolü.(Adminin izleme işlemi sınırsızdır)
- Kullanıcı ekleme ve kullanıcı hakları verme.
- Kullanıcı bilgilerinin güncellenmesi.
- Kullanıcı silme.
- Duyuru modülü.(Sadece site kullanıcılarının okuyabilecekleri duyuru sistemi)

2.1. Gerçek zamanlı web trafik kontrolü

Adminin hakları sınırsız olduğu için, hak sınırlaması olmadan web trafik kontrolünü istediği gibi yapabilir.

- İp numarasına göre gerçek zamanlı web trafik kontrolü
- Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü.
- Web adresine göre gerçek zamanlı web trafik kontrolü.
- Girilen kelimeye göre gerçek zamanlı web trafik kontrolü.

Bu modülün genel görüntüleri.

Online (Realtime) IP Numarası- Bilgisayar Hangi Web Sitelerine Giriyor?

IP Numarası Giriniz

Sorgula **Sil**

Online, IP Numarası ve NetMask ile WEB Sitesi Arama?

IP Numarası Giriniz **Subnet Mask Giriniz**

Sorgula **Sil**

Şekil 1 Web trafik tontrolü yapan modülün genel görüntüsü 1

Online olarak Hangi WEB ADRESINE Kimler Giriyor?

WEB Adresi Giriniz

Sorgula Sil

Online WEB ADRESI İcinde Kelime Arama

Aranacak Kelimeyi Giriniz

Sorgula Sil

Erhan YELİ © 2003 erhanyeli@hotmail.com

Şekil 2 Web trafik tontrolü yapan modülün genel görüntüsü 2

2.1.1. İp numarasına göre gerçek zamanlı web trafik kontrolü

Admin yazdığı ip numarasının şu an hangi sitelere girdiğini bu form sayesinde görebilir. Örneğin 10.8.2.72 numaralı ip'nin girdiği siteler aşağıdaki şekilde sorgulanır.

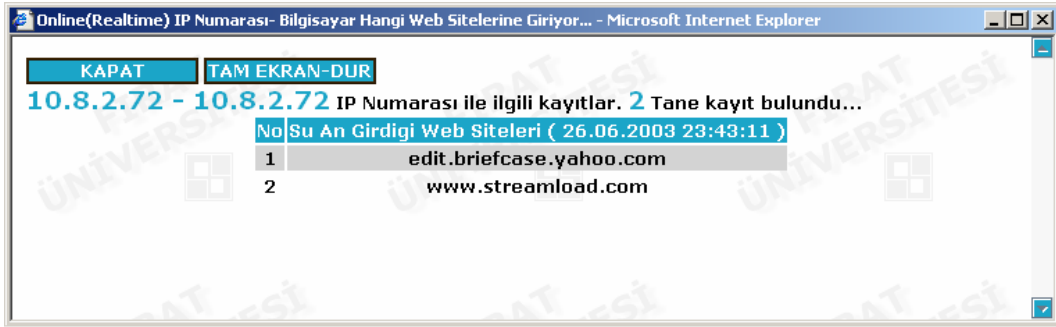
Online (Realtime) IP Numarası- Bilgisayar Hangi Web Sitelerine Giriyor?

IP Numarası Giriniz

Sorgula Sil

Şekil 3 İp numarasına göre gerçek zamanlı web trafik kontrolü

Bu sorgulama sonucu ařađıdaki gibi olur.

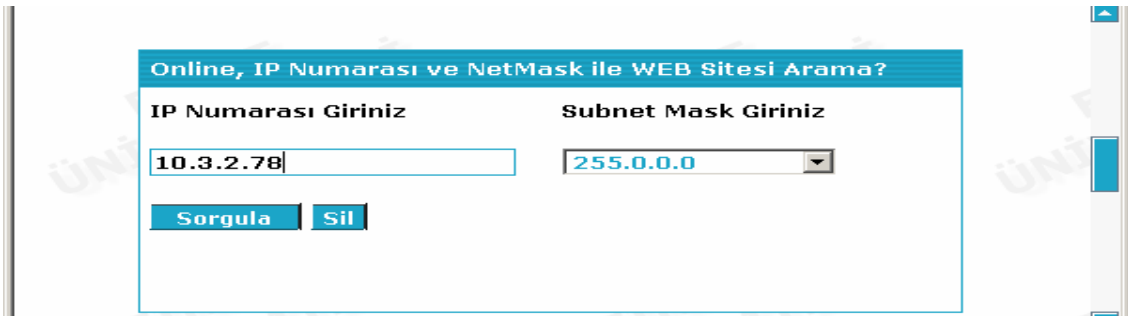


řekil 4 İp numarasına gre gerek zamanlı web trafik kontrol sonucu

2.1.2. Alt ađ maskesine gre gerek zamanlı web trafik kontrol

Girilen ip numarasının bulunduđu alt altdaki btn bilgisayarları ve bu bilgisayarların girdiđi internet adreslerini gerek zamanlı olarak listeler. nce ip numarası yazıp alt ađı seiyoruz(Seilebilen alt ađ adresleri : 255.0.0.0 – 255.255.0.0 – 255.255.255.0 – 255.255.255.255). Daha sonra gerek zamanlı olarak webde sorgu sonuları olur.

Ařađıda 10.3.2.78 ip numarasının bulunduđu alt ađla ilgili sorgulama yapıyoruz. Alt ađ maskesi 255.0.0.0 ‘dır.



řekil 5 Alt ađ maskesine gre gerek zamanlı web trafik kontrol

Bu sorgulama sonucu ařađıdaki gibi olur.

No	Web Sitesinin Adı	Web Sitelerine Giren Kullanıcılar (26.06.2003 23:35:21)	Bilgisayar Adı
1	www.ourworld.com	10.9.2.69	y6i2j0.firat.edu.tr
2	www.mustafaislamoglu.com	10.9.2.161	h2s5e1.firat.edu.tr
3	www.employment.harris.com	10.9.2.77	edemirciev.firat.edu.tr
4	www.ato.org.tr	10.8.2.253	10.8.2.253
5	squid.firat.edu.tr	10.3.2.78	hguler1.firat.edu.tr

řekil 6 Alt ađ maskesine gre gerek zamanlı web trafik kontrol sonucu

2.1.3 Girilen kelimeye gre gerek zamanlı web trafik kontrol

Formda girilen kelimenin getiđi web adreslerini ve bu web adreslerine giren kullanıcıların ip numarası-bilgisayar adlarını gsterir. rneđin “ . ” nın getiđi web adreslerini arayalım.

Online WEB ADRESİ İcinde Kelime Arama

Aranacak Kelimeyi Giriniz

řekil 7 Girilen kelimeye gre gerek zamanlı web trafik kontrol

Bu sorgulama sonucu aşağıdaki gibi olur.

No	Web Sitesinin Adı	İçinde Kelimesi Geçen Web Sitelerine Giren Kullanıcılar (26.06.2003 23:42:41)	Bilgisayar Adı
1	files.cc.cometsystems.com	10.9.2.21	standart
2	mail01.mail.com	10.9.2.21	standart
3	www.pgmusic.com	10.9.2.21	standart
4	edit.briefcase.yahoo.com	10.8.2.72	10.8.2.72
5	www.streamload.com	10.8.2.72	10.8.2.72
6	squid.firat.edu.tr	10.3.2.78	hguler1.firat.edu.tr

Şekil 8 Girilen kelimeye göre gerçek zamanlı web trafik kontrolü sonucu

2.2 Kullanıcı ekleme ve kullanıcı haklarını belirleme

Bu modülde kullanıcı bilgileri alınır. Kullanıcının siteden ne ölçüde yararlanacağını belirten kullanıcı hakları admin tarafından belirlenir.

Bu haklar aşağıdaki formların tamamını kullanıcıya gösterme veya belirli bir kısmını gösterme şeklindedir.

- İp numarasına göre gerçek zamanlı web trafik kontrolü
- Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü.
- Web adresine göre gerçek zamanlı web trafik kontrolü.
- Girilen kelimeye göre gerçek zamanlı web trafik kontrolü.

İp numarasına göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız ip kontrol hakkı vermelisiniz veya sadece belirli bir ip aralığı vermeniz gerekir.

Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız sınırsız sorgulama hakkı vermelisiniz veya sadece belirli bir ip ve alt ağ maskesi ile sorgulama yapmasına izin vermeniz gerekir.

Web adresine göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız sınırsız sorgulama hakkı vermelisiniz veya sadece belirli web sitelerinin adlarını aratma hakkını vermeniz gerekir. Web sitelerinin adları admin tarafından kullanıcı ekleme modülünden girilebilir.

Girilen kelimeye göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız sınırsız sorgulama hakkı vermelisiniz veya sadece belirli

kelimeleri aratma hakkını vermeniz gerekir. Kelimeler admin tarafından kullanıcı ekleme modülünden girilebilir.

IP sınırlama kontrolleri server üzerinde çalışan javascript ile yapılmıştır.

Kullanıcı ekleme modülünün ekran görüntüleri

The screenshot shows a user registration form with the following fields and values:

- Kullanıcı Adı:** Erhan
- Şifre:** 12345
- Adı:** Erhan
- Soyadı:** Yeli
- Email Adresi:** erhanyeli@hotmail.com
- Açıklama:** Sınırlı Kullanıcı....

Below the main form, there is a section for IP range control:

- IP Aralık Belirtme**
- Kullanılabilecek IP Aralığı:** 10.3.1.1 ile 10.3.1.255
- Sınırlama Yok**

Şekil 9 Kullanıcı ekleme 1

The screenshot shows the IP control and word control sections of the user registration form:

- IP - Netmask Kontrolü**
- Kullanılabilecek IP:** 10.7.7.7
- Netmask:** 255.0.0.0
- Sınırlama Yok**

Below this, there is a section for word control:

- Kelime Kontrol**
- Kelime Yazıp Enter'a Basınız:** xxx, yyy, zzz, oyun
- Kelime Sınırlaması Yok**

Şekil 10 Kullanıcı ekleme 2

WEB Adresi İzleyebilme

WEB Adresi Yazıp Enter'a Basınız

www.mynet.com
www.oyun.com
www.chat.com

WEB Sınırlaması Yok

Tamam Sil

Şekil 11 Kullanıcı ekleme 3

3. KULLANICI ARABİRİMİ

Kullanıcı, admin tarafından verilen haklara göre aşağıdaki sorgulamaları gerçek zamanlı olarak yapabilmektedir.

- İp numarasına göre gerçek zamanlı sorgulama.
- Alt ağ maskesine göre gerçek zamanlı sorgulama.
- Web adresine göre gerçek zamanlı sorgulama.
- Girilen kelimeye göre gerçek zamanlı sorgulama.

Örneğin Erhan kullanıcısının hakları yukarıda kullanıcı ekleme modülünde girilmiştir. Bu kullanıcı login olduktan sonra hakları ve bununla ilgili ekran görüntüleri aşağıdaki gibidir. Admin formlardan herhangi birini işaretlemeseydi o form kullanıcı arabiriminde gözükmeyecekti.

Bu formlardan herhangi birinde gerçek zamanlı sorgulama yaptığı zaman oluşan sonuçların ekran görüntüleri bölüm 2.1'de gösterilmiştir.

FIRAT ÜNİVERSİTESİ Suid Proxy İle Gerçek Zamanlı WEB Trafik Kontrolü

Kullanıcı Adı	<input type="text"/>
Şifre	<input type="password"/>
<input type="button" value="Giriş"/> <input type="button" value="Temizle"/>	

Şekil 12 Kullanıcı girişi

Şekil 13 'te kullanıcıya ayrılmış ip sınırları dışında ip sorgulaması yapamaz. Bu serverda çalışan javascript koduyla yapılmıştır. Ayrıca kendisine verilmiş olan ip ve alt ağ maskesi dışına çıkıp sorgulama da yapamamaktadır.

Online (Realtime) IP Numarası- Bilgisayar Hangi Web Sitelerine Giriyor?	
10.3.1.1 - 10.3.1.255 IP ARALIGINDA	
IP Numarası Giriniz	
<input type="text"/>	
<input type="button" value="Sorgula"/>	<input type="button" value="Sil"/>

Online, IP Numarası ve NetMask ile WEB Sitesi Arama?	
10.7.7.7 Sadece Yazabilirsiniz...	
IP Numarası Giriniz	Subnet Mask Giriniz
<input type="text"/>	<input type="text" value="255.0.0.0"/>
<input type="button" value="Sorgula"/>	<input type="button" value="Sil"/>

Şekil 13 Hakları sınırlandırılmış kullanıcı ekranı 1

Şekil 14 'te kullanıcıya adminin vermiş olduğu web adresleri dışında sorgulama hakkı tanınmamıştır.



Şekil 14 Hakları sınırlandırılmış kullanıcı ekranı 2

Şekil 15'te kullanıcıya adminin vermiş olduğu kelimeler dışında sorgulama hakkı tanınmamıştır.



Şekil 15 Hakları sınırlandırılmış kullanıcı ekranı 3

KAYNAKLAR

1. www.linux.org.tr
2. www.php.org.tr
3. www.php.net
4. www.linux-sevenler.de
5. www.belgeler.org
6. www.turk-php.com
7. www.gelecek.com.tr
8. www.zend.com
9. www.mysql.com
10. www.enderunix.org
11. www.w3.com
12. www.squid-cache.org
13. www.fazlamesai.net
14. www.programlama.com
15. www.sorucevap.com
16. www.wrox.com

KİTAPLAR

1. Özgür ÇAYCI, PHP ve MySQL
2. Kayra OTANER, PHP ve MySQL ile Web Yazılımı Geliştirme
3. Görkem ÇETİN, Bilgisayar Ağları ve Linux Ağ Yönetimi
4. T. H. CORMEN, Instruction To Algorithms