

I-Bekci Sisteminin Kampüs Ortamında Kullanımı

Abdullah Baykal

Dicle Üniversitesi Bilgi-İşlem Daire Başkanlığı, 21280-Diyarbakır
baykal@dicle.edu.tr

Özet: Günümüzde kampus ağlarının iç ve dış tehditlere karşı korunması , üniversiteler için en öncelikli sorunlardan biri haline gelmiştir. Ağın güvenli bir şekilde çalışmasının sağlanması ve kullanıcılara güvenli bir hizmet sunulabilmesi için büyük bir emek ve zaman harcanmakta bunun için çeşitli ağ güvenlik cihazları ve programları kullanılmaktadır. Bu bildiride, Türkiye’de geliştirilen Bilgi iletişimi ve Güvenliği cihazı olarak kullanılan i-bekçi ‘nin kampus ortamlarında kullanımı anlatılacaktır.

Anahtar Kelimeler: Ağ Güvenliği , i-bekçi, Güvenlik Duvarı, Yönlendirici

Abstract: Nowadays, protection of campus network against internal and external dangers have become the initial problem for universities. To supply functioning of network safely and serve safe connection to users,a great deal of effort and time is spent,so different network security devices and programs are used.In this report using of i-bekçi,which is developed in Turkey and used as Information Communication and Security Appliance in campus,will be introduced.

Keywords: Network safety, i-bekci, Firewall, Router

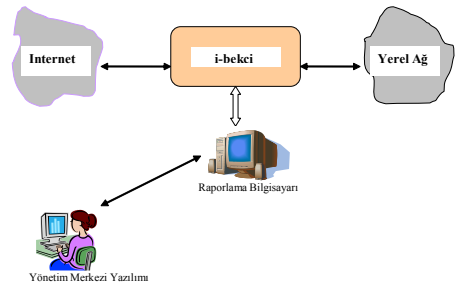
1. Giriş

i-bekçi cihazı kurumların ihtiyaçlara göre düzenlenmiş farklı 6 modeli bulunmaktadır. Modeller ibc-500, ibc-1000, ibc-2000-a, ibc-2000-ct , ibc-2000-lb ve ibc-3000-gk şeklindedir[1]. Farklılıklar daha çok cihazın teknik özelliklerinden kaynaklanmakta , tüm modellerde yazılımlar ve işlevsellik aynı olmaktadır. i-bekçi işletim sistemi OpenBSD tabanlıdır[2]. İşletim sistemi donanımsal sürücüler , yönetim, raporlama ve diğer yazılımları barındırmaktadır. Sistem komut satırında , çalıştır, durdur, göster, güncelle gibi Türkçe komutlar kullanılabilir. İ-bekçi ile aşağıdaki uygulamalar yapılabilir.[3]

- Yönlendirici
- Güvenlik Duvarı
- Ölçeklendirilebilirlik
- Yük Dengeleme
- Haciyatmaz
- İçerik Denetimi

- Uyarı Mekanizması
- Sanal Ağ Desteği
- P2P Kesici
- Saldırı Tespit ve Önleme Sistemi

2. Kurulum



Şekil-1: i-bekçi kurulum yapısı

Kurulum 3 adımdan oluşmaktadır (şekil.1) bunlar;

1. i-bekçi cihazının kurulumu, bu genellikle yerel ağ ile dış ağ (internet) arasına olmaktadır.

2. i-bekçi üzerinden geçen verilerin raporlama amacıyla saklanması için raporlama bilgisayarı kurulumu,
3. Ayarlamalar ve raporlamalar için bir bilgisayar üzerinde kurulacak Yönetim Merkezi yazılımı

3. I-Bekci Yönetim Merkezi

Yönetim Merkezinin grafiksel ara yüzü yardımıyla i-bekci'ye ulaşılabilir, ayarlar yapılabilir, anlık veya geçmişe yönelik raporlar görüntülenebilir (Şekil-2). Program çalıştırıldığında önce ağda mevcut i-bekçileri tespit eder. Seçilen i-bekçi için,

- Anlık Veri Gösterciler
- Veritabanı (VT) Gösterciler
- Olmak üzere 2 temel grup için raporlar düzenlenebilir. Anlık Veri Gösterciler, çevrim-içi verilerin raporlandığı



Şekil-2. Yönetim Yazılımı

Araçlardır[4]. Veritabanı(VT) Gösterciler ise, veritabanındaki kayıtlı bilgilerin, verilen tarih aralığında sorgulanması sonucu oluşturulan raporların alınabildiği araçlar topluluğudur. Bu araçlar aşağıdaki verildiği gibi Anlık Veri Gösterciler ve Veritabanı(VT) Gösterciler olmak üzere 6 'şar adettir[4].

- Durum Göstercisi
- Erişim Göstercisi
- Günlük Göstercisi
- Başarım Göstercisi
- Kuyruk Göstercisi
- Uyarı Göstercisi

Yönetim Yazılımı üzerinden, raporlama araçları dışında aşağıdaki yazılımlar çalıştırılmaktadır;

- Kural Üretici
- P2P Düzenleyicisi
- Güvenli İletişim Uçbirimi

3.1. Durum Göstergesi

Kaynak IP	Oturum	Başl	Dış	M	P	Paket	Paket
10.1.10.2	1	4.2M	1K	2.5M	4K	100512	150640
95.112.5	1	2.2M	3K	180.3M	29K	53936	107332
10.1.14.96	156	7.7M	1K	133.7M	37K	61883	96154
10.1.80.9	1	827K	1K	33.6M	27K	14130	23758
10.2.3.60	277	5.2M	7K	32.0M	28K	17323	24793
10.2.1.55	1	687K	3K	32.3M	13K	15043	21510
10.2.4.219	170	1.1M	3K	20.9M	23K	21044	28126
10.1.10.65	1	1.2M	3K	76.7M	13K	21130	28790
10.1.3.20	348	14.2M	19K	20.3M	11K	20847	22348
10.1.10.11	1	427K	3K	18.6M	13K	1842	12270
10.1.10.1	242	17.7M	23K	16.2M	12K	22342	28775
10.1.10.87	1	387K	3K	14.0M	8K	8271	12219
10.1.34.57	26	274K	3K	14.0M	3K	8137	14115
10.1.1.21	2	18.7M	27K	1.3M	23K	29138	18000
10.1.34.1	2	269K	1K	1.26M	53K	6181	8454
10.2.10.1	12	294K	3K	1.1M	8K	8474	11704
10.1.11.77	57	259K	1K	1.0M	33K	5530	8031
10.1.11.1	1	283K	3K	1.0M	8K	5657	8145
10.2.4.25	18	235K	3K	1.0M	23K	5314	7054

Grup Sayısı: 575 Veri miktarı: 17,0259

Şekil-3: Durum Göstergesi Tablosu

Durum Göstergesi penceresinde (şekil-3) anlık olarak oluşan trafik listelenmektedir, bunlar

- Durumu oluşturan Kaynak IP adresi
- Bu IP adresine ait ; Oturum sayısı, indirilen verinin byte cinsinden toplam büyüklüğü, saniyede indirilen veri miktarı, gönderilen paket ve veri miktarı gibi bilgiler tablo olarak alınabilmektedir. Yine bu tabloda kay-

nak bir IP üzerine çift tıklayarak , ilgili IP nin oturum ayrıntısı alınabilir veya istenirse tablo bilgileri grafiksel olarak istenebilir.

3.2. Erişim Göstergesi

Bu pencerede i-bekçi üzerinden geçen trafiğin, paket eleği kurallarına göre geçişine izin verilmesi yada durdurulması ile ilgili bilgiler verilir. Erişim Göstergesinde bulunan Süzgeç yardımı ile verilerin istenilen kriterlere göre süzülerek gösterilmesi sağlanabilir.

3.3. Günlük Gösterici

Bu pencerede i-bekçi sistem bilgileri anlık olarak görülebilir. Bunlar ;sistem değişiklikleri, ssh bağlantıları ve p2p kesici bilgileri ve benzeri gibi bilgilerdir.

3.4. Başarım Gösterici

Bu pencerede, İşlemci, bellek, Paket eleği ve ara birimlerin durumları listelenmektedir (şekil.4). Listedeki bilgilerden hattın ne kadar kullanıldığını giriş ve çıkış düzeyinde anlık görüntülenebilir.



Şekil-4: Başarım Göstergesi Tablosu

3.5. Kuyruk Göstergesi

Bu pencerede i-bekçi üzerindeki kuyruklarla ilgili veriler grafiksel olarak görüntülenir.

3.6. Uyarı Gösterici

Bu pencerede i-bekçi'ye yada koruduğu ağa gelen saldırılar konusunda bilgi verir. Bu saldırılar, yanlış/doğru ssh bağlantıları, dosya saldırısı, durum bilgileri, servis tarama saldırıları gibi bir çok uyarı görüntülenebilmektedir. Bu uyarılar , Birinci (düşük) hatalı uyarılar, ikinci (orta) şüpheli hareketler ve üçüncü (yüksek) izinsiz giriş saldırılar, seviyelerde olmaktadır. İsteğe bağlı olarak bu uyarılar ,mail ya da fax yolu ile sistem yöneticisine bildirilmektedir.

3.7. P2P Düzenleyicisi

Bu düzenleyicisi ile i-bekçi üzerinde gelen p2p programların imzalarına, istenilen imzalar eklenerek söz konusu imzaların bulunduğu iletişim engellenebilir.

3.8. Kural Üretici

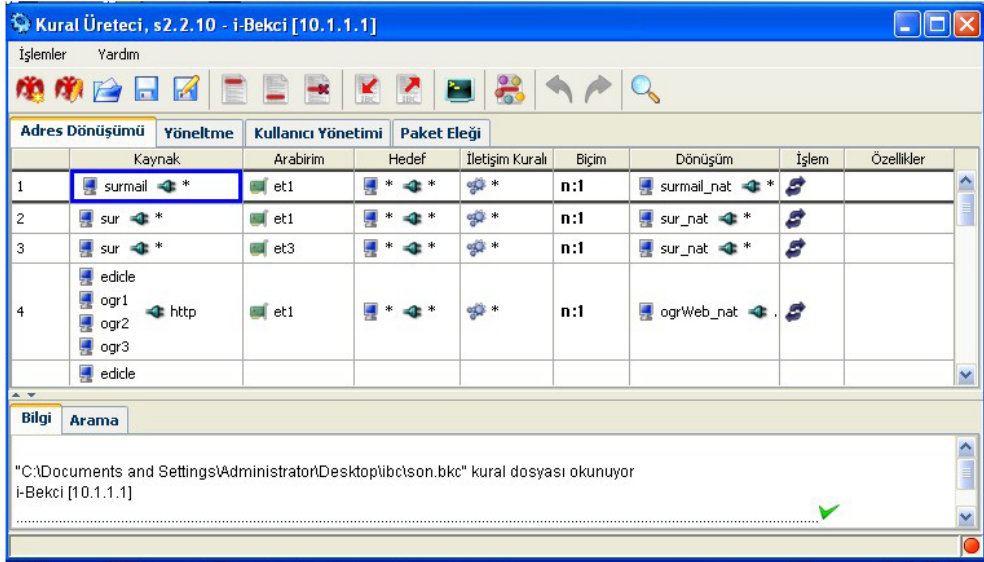
Kural Üretici (şekil.5), i-bekçi cihazı ile beraber gelen Paket Eleğinin kullanılabilmesi için gereken bir yazılımdır. Kural Üretici Java ile yazılarak platformdan bağımsız hale getirilmiştir

4. Kampus Ortamında Kullanımı

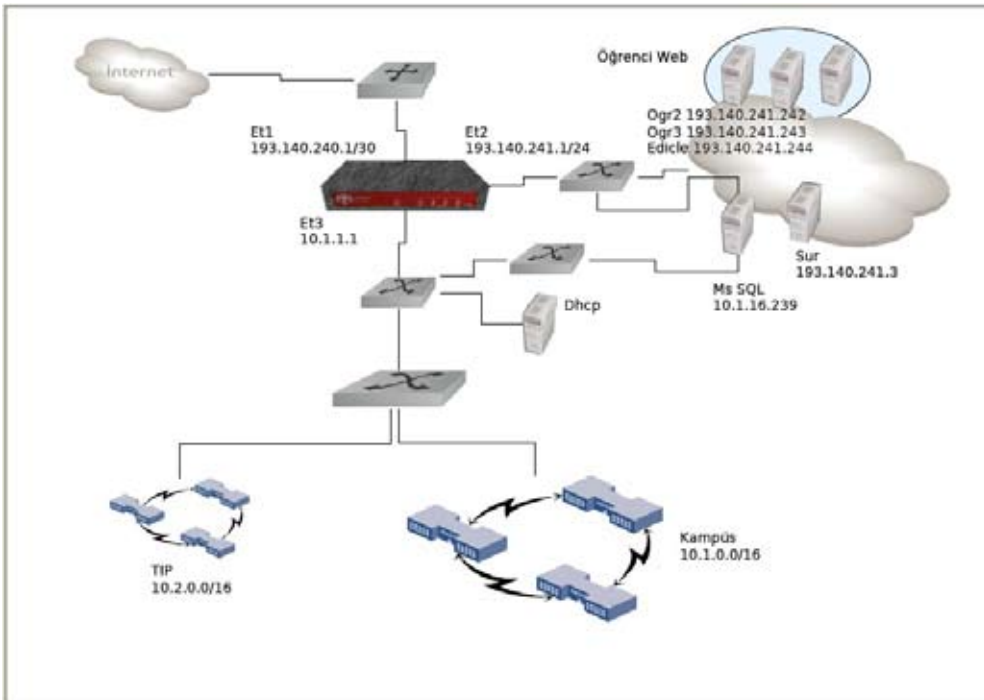
Dicle kampusun de i-bekçi uygulaması şekil-6 da verildiği gibi düzenlenmiştir. Kullanılan uygulamalar aşağıda verilmiştir.

- Adres Dönüştürücü : Kampus ortamında kullanılan sanal ip ler çıkışta NAT yapılarak gerçek ip dönüştürülmektedir.
- Hacıyatmaz : Öğrenci otomasyonunda kullanılan sunuculara gelen trafiği dengeli bir şekilde i-bekçi üzerinden dağıtılmaktadır.
- Raporlama araçları kullanılarak ağ güvenliği konusunda anlık ayrıntılı bilgi elde edilmekte ve geçmişe yönelik olarak birçok kritere göre sorgulamalar yapılarak istenilen raporlar alınabilmektedir.
- İmza yönetici (p2p düzenleyicisi) kullanılarak istenilmeyen trafik ağ üzerinde önlenmektedir.
- Gelen mail'lerin virus ve spam taraması için i-bekçi üzerinden smtp(25 port) trafiği , Virus/antispam cihazına yönlendirilmektedir.

- Sunucu bilgisayarlara sadece istenilen portlardan ulaşılması sağlanabilmektedir
- Saldırı önleme ve tespit sistemi[5] ile istenmeyen trafik tespit edilerek TCP_baglanti_kes, IP_durdur, PE_durum_sil vb. komutlarla önlenmektedir.



Şekil-5. Kural Üreteci



Şekil-6: Dicle Ağ yapısı

5. Sonuç

Sonuç olarak Türkiye’de geliştirilen i-bekçi cihazı, kampus ortamlarında ağ güvenliği için kullanılabilen , anlık ve geçmişe yönelik güçlü raporlama olanakları bulunan bir güvenlik cihazı olduğu görülmektedir.

6. Kaynaklar

- [1]. i-bekçi modeller dökümanı
- [2]. <http://www.openbsd.org>
- [3]. i-bekçi/z-sistem. <http://www.z-sistem.com>
- [4]. i-bekçi Bilgi İletişimi ve Ağ Güvenliği cihazı El Kitabı
- [5]. i-bekçi Saldırı Tespit Sistemi El kitabı