

i-bekçi ■ Bilgi İletişimi ve Güvenliği Cihazı

Teknik Tanıtım Kitapçığı

- ◆ Yönlendirici
- ◆ Güvenlik Duvarı
- ◆ Türkçe Yazılım Araçları
- ◆ 7/24 Sürekli Destek
- ◆ Ölçeklenebilirlik
- ◆ Kriptolu İletişim, GSA
- ◆ Yedekli Çalışma
- ◆ Geniş Alan Ağı Bağlantı Yedekleme
- ◆ Metro Et. / ADSL / V.35 / E1 / E3
- ◆ Yük Dengeleme
- ◆ Hacıyatmaz
- ◆ İçerik Denetimi
- ◆ Trafik Önceliklendirme
- ◆ Uyarı Mekanizması
- ◆ Saydam Çalışma
- ◆ IP üzerinden Ses Taşıma
- ◆ Sanal Ağ desteği



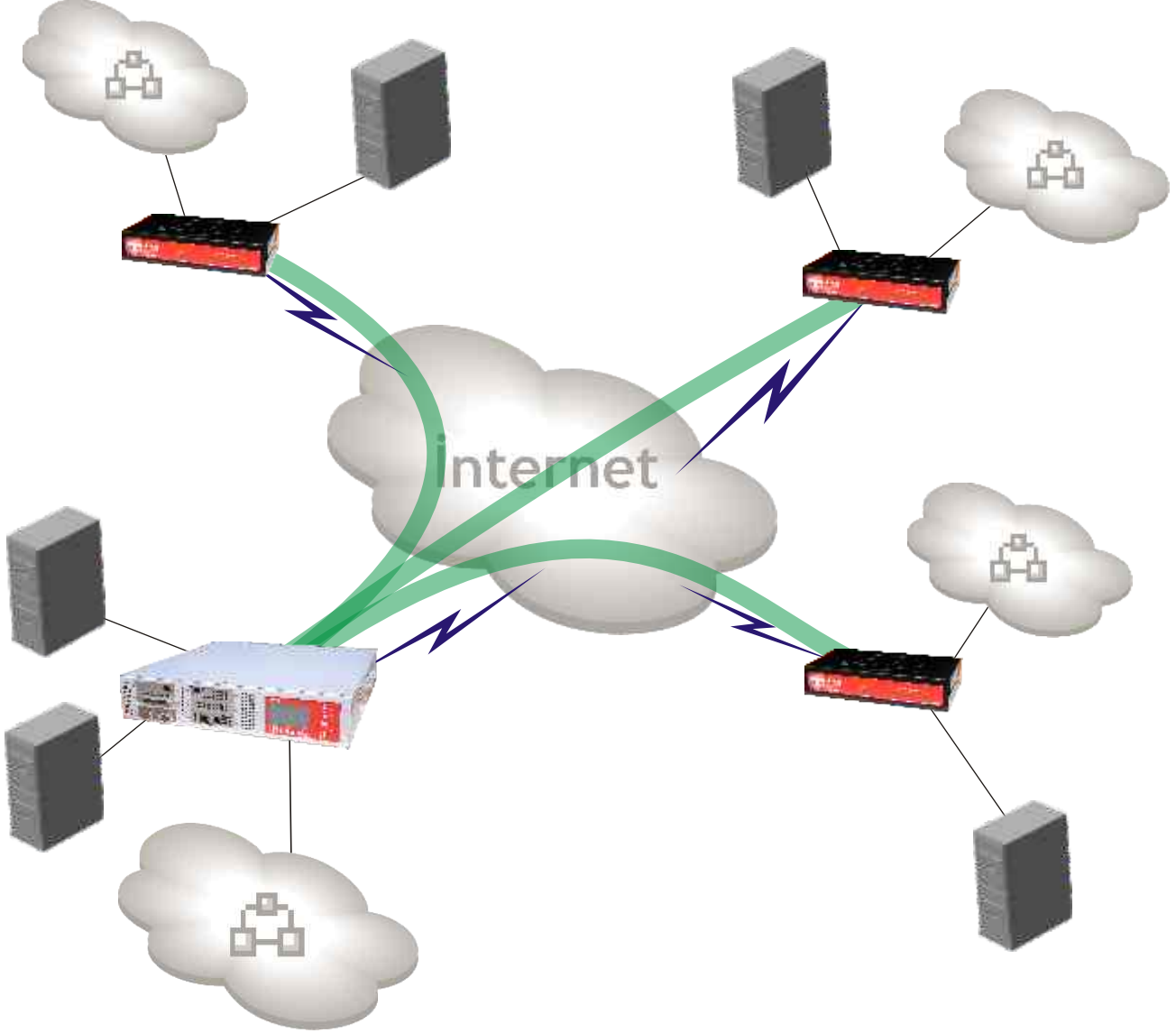
i-bekçi

z-sistem

z-sistem

Bilgi ve İletişim Güvenliği i-bekçi'ye Emanet.

www.turk.internet.com



Ulusal bilişim güvenliğine i-bekçi.

www.hurriyet.com.tr

- i-bekçi, Z-Sistem'in tescilli markasıdır.
- i-bekçi , Ankara'da tasarlanmakta ve üretilmektedir.
- Kitapçık bilgilendirme amaçlıdır. Kitapçığın içeriği, haber verilmeden değiştirilebilir. (Güncel bilgilere www.z-sistem.com adresinden ulaşılabilir).
- Kullanılan diğer markalar kayıtlı kendi sahiplerine aittir.

Belge Sürüm No: 4.1

i-bekçi İşlevsellik Haritası

1. i-bekçi Donanımı

- i-bekçi Bileşenleri
- i-bekçi Modelleri
 - ibc-500
 - ibc-750 *
 - ibc-1000
 - ibc-2000
 - ibc-2000-ct
 - ibc-2000-lb
 - ibc-3000-gk
 - ibc-4000-ml

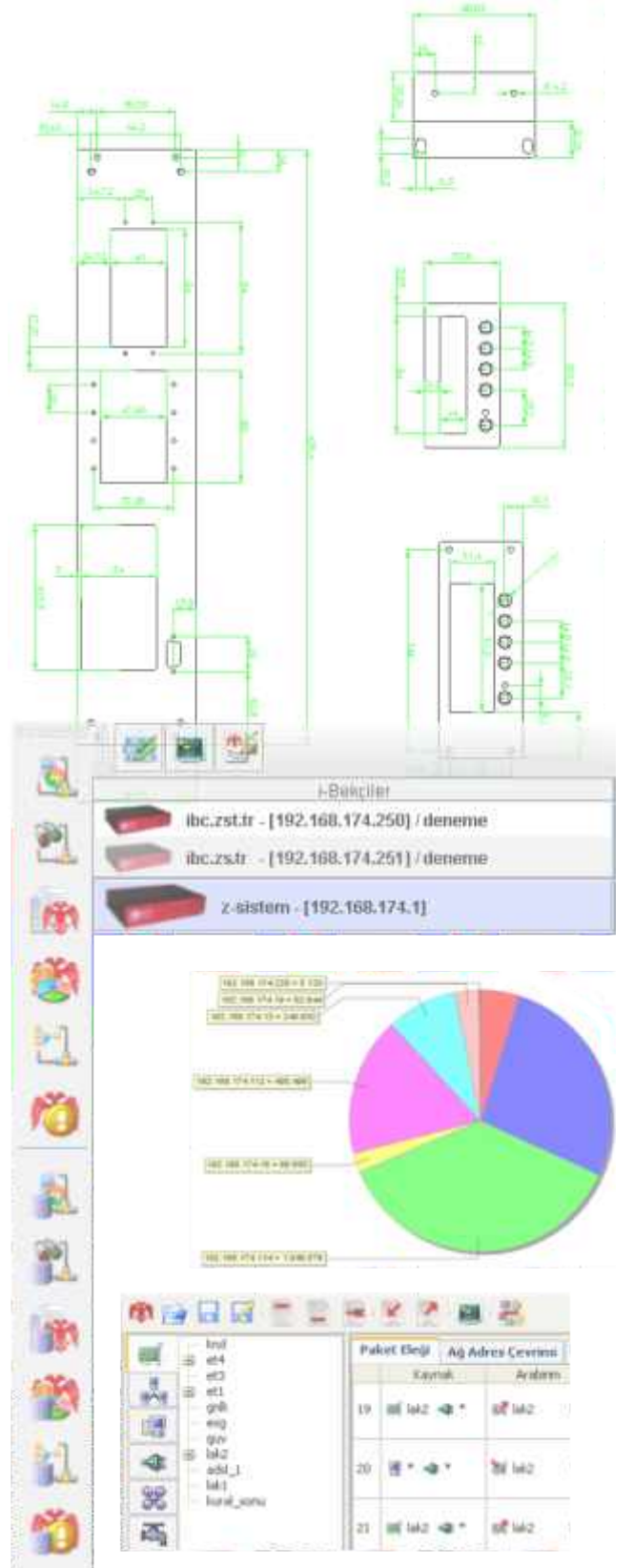
2. i-bekçi İşletim Sistemi

- Komut Satırı Kullanıcı Arayüzü
- Hacıyatmaz
- Paket Eleği
- Saldırı Tespit ve Önleme Sistemi
- Rapor Üreticiler, İstatistik Sağlayıcılar
- Güvenli Sanal Ağ
- Trafik Önceliklendirme
- Küme
- IP Trafiğini İzleme
- Sanal Ağ, 802.1q
- Ses İletişimi *

3. i-Bekci Yönetim Merkezi

- Kural Üretici
- Web Eleği *
- İmza Yönetici/Paket İşleyici
- Raporlama Araçları
- Kullanıcı Yönetimi

4. i-Bekci GSA istemci



*) 2006 ikinci yarısından sonra planlanan

Giriş

i-bekçi Bilgi İletişimi ve Güvenliği (BiG) Cihazı, Donanım, Yazılım, Destek, Danışmanlık ve Eğitimden oluşan bir üründür.

i-bekçi;

- Endüstriyel donanım,
- IP yönlendirici,
- Güvenlik duvarı,
- Güvenli Sanal Ağ (GSA) sonlandırıcı,
- Kuyruk yönetimi (trafik önceliklendirme),
- Yedekli çalışma,
- Yük dengeleme,
- Geniş alan ağı bağlantı yedekleme,
- İçerik denetimi,
- Hacıyatmaz,
- Uyarı mekanizması,
- Saydam çalışma,
- Kullanıcı yönetimi,
- GSA istemci

işlevselliklerini bünyesinde barındırmaktadır.

i-bekçi, endüstriyel özellikteki donanım, 7/24 güvenilirlik, sürdürülebilirlik ve kolay yönetilebilirlik ilkelerine göre üretilmiştir.

AR-GE süreci sonunda ve sahada denenerek üretilen i-bekçi, daha sonra gelişimini özel şirket ve kamu kuruluşlarının ihtiyaçları doğrultusunda sürdürmüştür. Her biri mühendislik ürünü olan donanım ve yazılımlar, e-bilgi politikaları ve iş süreçleri göz önünde bulundurularak gerçekleştirilmiştir. e-Bilgi güvenliği uygulayıcıları, kurumsal e-güvenlik politikalarını i-bekçi kullanarak oluşturabilmektedirler.

Ürün eğitimi, üretim bilgisi ile Türkçe olarak verilmektedir. Ürün şu an sadece Türkçe dil desteğine sahiptir.

i-bekçi'nin ayırdedici bazı özellikleri

- Sınırsız kullanıcı *
- Sınırsız oturum *
- Sınırsız GSA tüneli *
- Sınırsız Sanal Ağ desteği *
- İki yıl donanımsal garanti, yama ve yazılım güncellemeleri **
- Yüksek çalışabilirlik özelliği ***
- Ölçeklenebilirlik
- LCD gösterge paneli (ibc-1000 serisi ve altı hariç)
- Türkçe bir cihaz olması, bakım/destek ve öğrenme maliyetlerinin düşük olması
- Yerel üretici firma avantajları
- Çözüm ortağı üzerinden 7/24 destek,
- e-Güvenlik, IP Yönlendirici ve Ses özelliklerini bünyesinde barındırması,
- Donanımsal arızalarda, 1-2 iş günü içinde ürün/parça temini +

şeklindedir.

* Donanım elverdiği kadar.

** Yazılım güncellemeleri ve yamalar donanım güncellemesi gerektirmemelidir.

*** Yedekli çalışma tüm ürünlerde, yüksek çalışabilirlik özelliği ibc-2000 ve daha büyük seriler için geçerlidir.

Tüm ürünlerde kalıcı bellekler yonga şeklindedir ve elektrik kesintilerinde veri kaybetmezler.

+ Garanti süresi boyunca, donanımsal arıza oluşması durumunda, 1-2 iş günü içerisinde, ya arızalı ürünün yerine yenisi, ya da ürün tamir edilinceye kadar muadili bir ürün müşteriye gönderilir.

1. i-bekçi Donanımı

a) i-bekçi Bileşenleri

i-bekçi donanımını oluşturan temel ve seçimlerlik bileşenler:

- Ölçeklenebilir işlemci, bellek ve kalıcı bellek
- Donanımsal zamanlayıcı ve ısı algılayıcılar
- Donanımsal Kripto Bileşeni
- LCD kumanda paneli
- Yerel Alan Ağı arabirimleri
 - a) Ethernet 10/100/1000TX, GigaFX, GigaSX
 - b) Telsiz *
- Geniş Alan Ağı arabirimleri
 - a) V.35, E1, kanallı E1, E3
 - b) Adsl, g.Shdsl *
- Metro Ethernet
- IP-Ses kartı (FXO/FXS) *
- Endüstriyel şase
- Endüstriyel yedekli güç kaynağı
- Yedekli pervane

b) i-bekçi Modelleri



ibc-500 : Üzerinde standart dört adet 10/100 Mbit ethernet arabirimi vardır.



ibc-1000 : Üzerinde dört adet 10/100 Mbit ethernet arabirimi ve bir adet V.35, E1, Adsl vb. için genişleme yuvası vardır.



ibc-2000 : Üç adet 10/100/1000 Mbit ethernet arabirime sahiptir. İki adet genişleme yuvasına sahiptir.



ibc-2000-Ct : İki adet 10/100 Mbit ethernet arabirime sahiptir. 1u yüksekliğindedir ancak üç adet genişleme yuvası sunar. Yedekli pervane ve güç kaynağı standarttır.



ibc-2000-Lb : İki adet 10/100 Mbit ethernet arabirime ek olarak dört adet genişleme yuvası sunar. Yedekli pervane ve güç kaynağı standarttır.



ibc-3000-Gk : iki adet 10/100 Mbit ethernet arabirime ek olarak yedi adet genişleme yuvasıyla yüksek ölçeklenebilirliğe sahiptir. Yedekli pervane ve güç kaynağı standarttır.

*) 2006 ikinci yarısından sonra planlanan

2. i-bekçi İşletim Sistemi

- Donanımsal sürücülerini barındırır.*
- IP ve IPSEC yönlendirme yapar.
- Uzaktan güncellenebilir.
- Yönetim, raporlama ve diğer yazılımları barındırır.
- TCP/IP, IPSEC, Köprü, Tünel, Eternet (CSMA/CD), PPP, cHDL, F/R, 802.1q, 802.11, PPPoE, MPOA iletişim kurallarını barındırır.

a) d5k, Komut Satırı Kullanıcı Arayüzü

- d5k, komut satırından i-bekçi işlevselliğinin yönetimini sağlar, uzaktan bakımı kolaylaştıran bu özellik ayrıca seri yönetim arabiriminden i-bekçi'nin yapılandırılmasını da sağlar.
- Türkçe arayüzü, kolay kullanım ve çabuk öğrenme sağlar.
- Metin tabanlı ayarların saklanması ve taşınması çok kolaydır.
- Özellikle donanımın yapılandırılmasını sağlar (Eternet-TX-SX, Metro Eternet, FXS ses, ADSL, V.35, E1, Kanallı E1 ve E3 arabirimleri, kripto hızlandırıcılar).
- Sunucu yazılımların ayarlanmasını sağlar.
- Diğer ağ cihazlarına erişimi sağlar (ping, telnet vb. gibi).
- i-bekçi'nin uzaktan yönetimine yönelik yapılandırmayı sağlar.
- İletimini sağladığı TCP/IP trafiğinin izlenmesini sağlar (Sniffer).
- Kriptolama işlemlerini yönetir (IPSEC).
- Sanal ağlar oluşturabilir ve bunları yönetir (VLAN).
- Güvenlik politikaları oluşturulabilir.
- DHCP sunucu ve istemci ayarlarının yapılmasını sağlar.
- TCP/IP ve köprü yapılandırmasını sağlar.
- i-bekçi işletim sistemini ve kendisini güncelleyebilir.
- Kurumsal güvenlik politikalarını güncelleyebilir.
- Servis veren yazılımları ve ayarlarını güncelleyebilir.
- i-bekçi işlevselliğinin istatistiki verilerini sağlayabilir.
- Gerçekleştirilen yapılandırma işlemlerini kayıt edebilir.

```

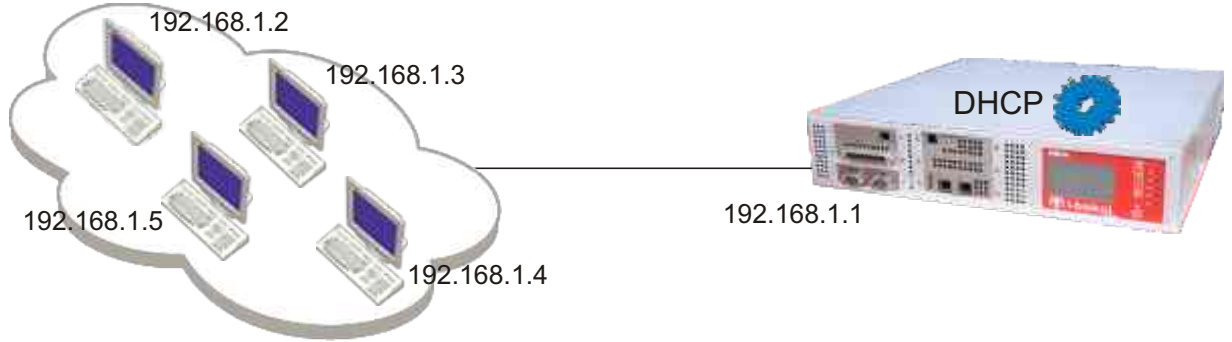
i-Bekçi Uçbirim Ekranı - v2.2.2
Dosya Düzenle Görünüm Araçlar Yardım
zsystem/yet
zsystem(##)/arb et3
zsystem(arb-et3)/ip 192.168.1.2/24
zsystem(arb-et3)/çık
zsystem(!)/çalıştır basun 192.168.1.5
paketler 192.168.1.5 adresine yönlendirildi ...
192.168.1.5 paketler gönderiliyor...
zsystem(!)/pe etkinleştir
zsystem(!)/sakla
zsystem(##)/
192.168.174.250:22 | ibekci | Bilinmeyen | Bağlantı Kuruldu

```

*) OpenBSD Tabanlıdır

DHCP Sunucu

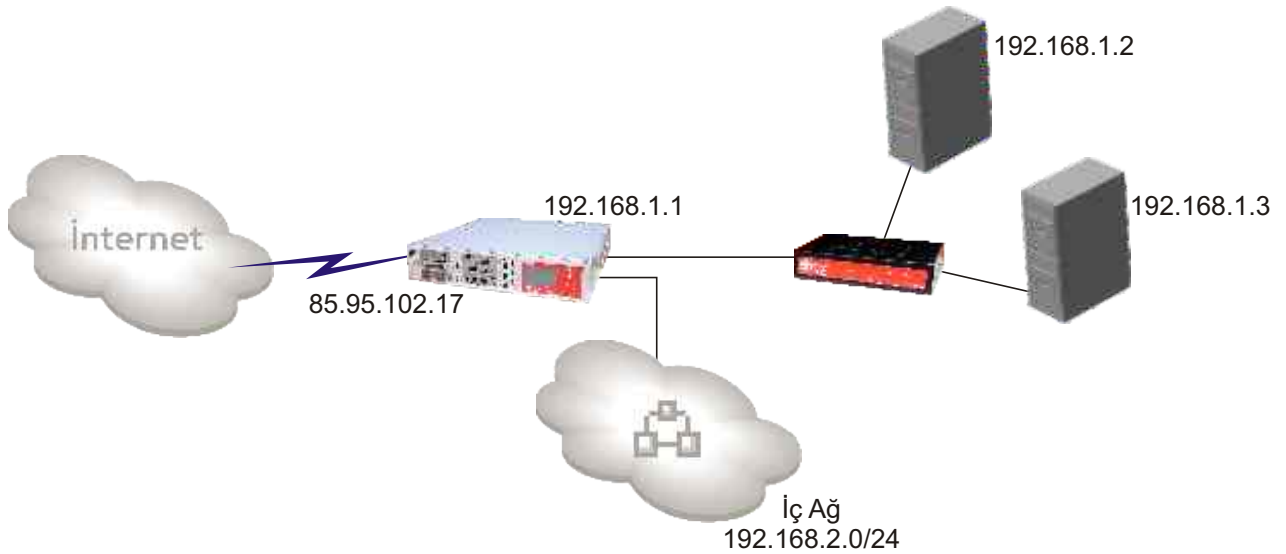
- i-bekçi koruduğu ağlar için aynı zamanda DHCP sunucu olarak çalışabilir.
- DHCP bilgilerinden, öntanımlı yönlendirici, isim sunucular ve IP adreslerini dağıtabilir.
- Koruduğu ağlar arasında DHCP istemlerini iletebilir (deneme aşamasında).



- i-bekçi'nin DHCP sunucu olarak çalışması

Saydam Çalışma

- i-bekçi, köprü olarak saydam çalışabilir. Bu sayede varlığı belli olmadan koruma yapabilir.
- Üzerinden geçen trafik için bir (yönlendirici) atlama noktası olarak görünmeden çalışabilir.
- Fazladan anahtarlama cihazına ihtiyaç duymadan, i-bekçi üzerindeki arabirimleri aynı ağdaymış gibi birleştirir (bir anahtarlama cihazı gibi davranabilir).
- Yeni bir ağ yapılandırmasına ihtiyaç duyulmadan, ağa güvenlik duvarı eklemeye olanak verir.
- Saydam çalışırken, üzerinde IP bulunmamasına rağmen, tam bir güvenlik duvarı olarak işlevini sürdürebilir.



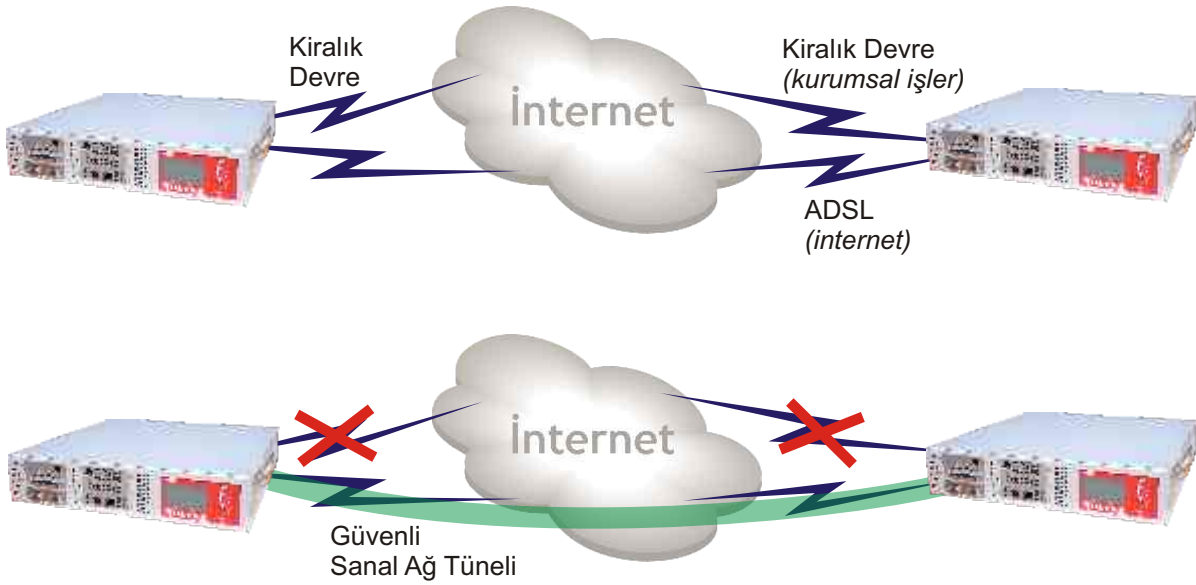
- i-bekçi'nin saydam çalışarak, güvenlik duvarı işlevini yerine getirmesi

b) Haciyatmaz

- Haciyatmaz, i-bekçi'nin işlevselliğinin belli durumlara göre programlanabilmesini sağlar. Bu sayede yönetici müdahalesi gerektiren durumlarda yapılan işlemler, i-bekçi üzerinde programlanmış olur ve sistem yöneticisi müdahalesine gerek kalmadan, benzer durum oluştuğunda i-bekçi tarafından yapılmış olur.
- Haciyatmaz ile i-bekçi'ye kazandırılmış olan ayarlama dilinin kullanımıyla, i-bekçi'nin farklı durumlardaki davranışı belirlenir. Kabuk ile sunulan tüm işlevsellik kullanılabilir.
- i-bekçi yöneticileri daha önceden karşılaşılmış durumları Türkçe olarak programlayabilirler.

Örnek Haciyatmaz yapılandırması :

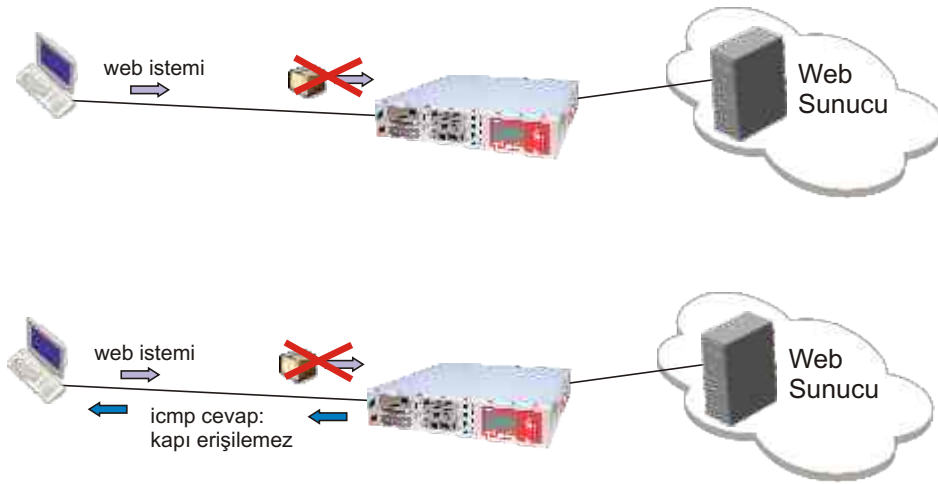
```
eğer 1.1.1.1 erişilebilir ve durum ed 1 ise {
    yönlendir 172.16.1.0/24 sil
    yönlendir 172.16.1.0/24 1.1.1.1
    durum = 1;
};
```



- Bu örnekte, kurumsal işler, kiralık devre üzerinden yapılırken, internet bağlantısı ADSL üzerinden verilmektedir. Haciyatmaz, kiralık devrede bir bağlantı sorunu çıktığında, kurumsal işlerin trafiğini hiç aksatmadan, ADSL hat üzerinden, interneti kullanarak kuracağı kriptolu bağlantıya taşıyacaktır.

c) Paket Eleği

- i-bekçi paket eleği, TCP/IP tabanlı olarak erişim denetimi sağlar.
- Durum korumalı çalışabilir ve TCP/IP iletişim kuralının denetimini sağlar.
- Ağ adres dönüşümü, kapı ve IP yöneltme işlemlerini yapar.
- IP birleştirme-parçalanma özelliklerini, i-bekçi'nin koruduğu ağlar için arabirim bazında yapabilir.
- Arkasındaki ağları sahte IP adresi erişimlerinden koruyabilir.
- TCP/IP iletişim kuralı parametrelerini, bağlantı sayılarını kural bazlı olarak değiştirebilir.
- TCP/IP iletişim kuralı ailesi adresine göre IP paketlerini geçirir veya durdurur.
- IP iletişimini TCP ve/veya ICMP mesajı döndürerek durdurabilir.
- IP paketlerini belirli amaçlar için farklı adreslere kopyalayarak veya yön değiştirerek geçirebilir.
- Paket eleme işlemlerini yaparken günlük bilgisi üretir.



- Paket eleği ile normal ve cevaplı durdurma

d) Saldırı Tespit ve Önleme Sistemi

- i-bekçi'nin koruduğu ağlara karşı çeşitli IP saldırılarını oluşurken tespit eder.
- Bazı saldırı türleri ötanımlı olarak durdurulur.
- ssh alt sistemi çalıştırabilen her harici güvenlik sisteminin kullanabileceği sts/sös mekanizması ile istenen IP adresleri durdurulabilir, tcp bağlantıları koparılabilir, oluşmuş paket eleği durumları silinebilir, durdurulmuş adresler listelenebilir ya da tüm uygulanmış kurallar kaldırılabilir.

e) Rapor Üreticiler, İstatistik Sağlayıcılar

- i-bekçi üzerinde çalışan rapor üreticiler, istatistik ve değerlendirme verisi üretirler. Bu veriler kayıt ve değerlendirme amaçlı olarak Raporlama Sunucusuna gönderilir. Raporlama kayıt yazılımları bir raporlama bilgisayarında değerlendirilebileceği gibi birden fazla hiyerarşik rapor değerlendirme sunucusu da kullanılabilir.

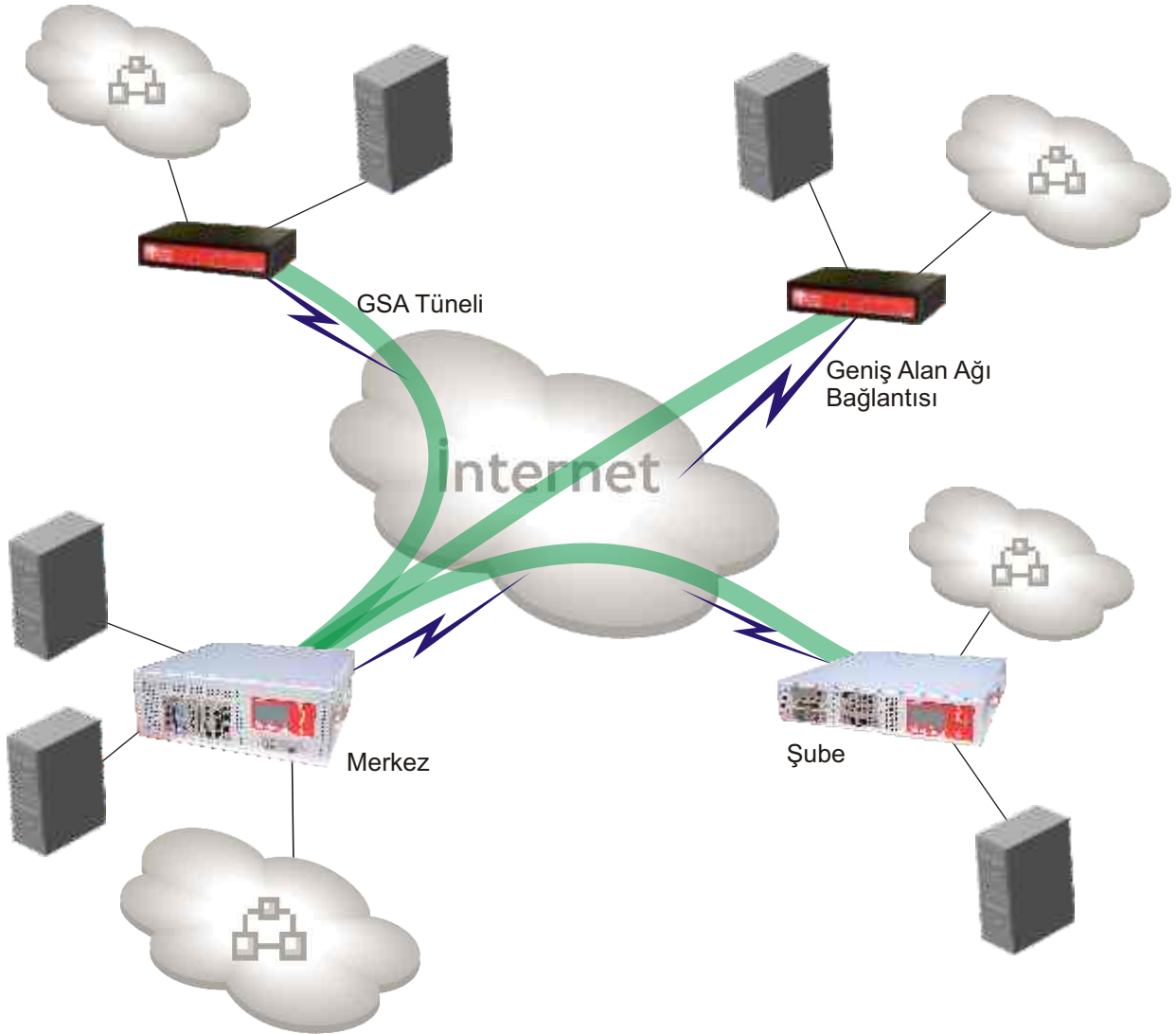
Üretilen raporlar:

- Başarım verileri,
- Erişim verileri,
- IP iletişim durumları,
- Trafik önceliklendirme (kuyruk) verileri,
- Yapılandırma ve diğer işlemlerin günlük verileri,

kaydedilip, izlenebilir.

f) Güvenli Sanal Ağ (GSA), Kriptolu İletişim

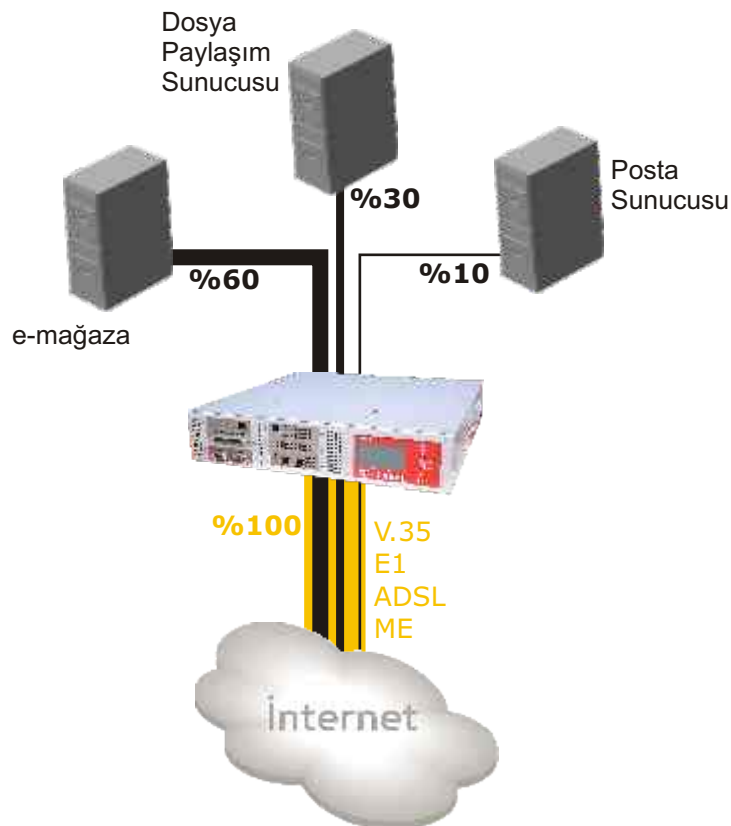
- Güvenli sanal ağlar için gerekli olan alt bileşenlerin kolayca tanımlanmasını sağlar. IPSEC ve IKE desteği ile GSA gerçekleştirilir.
- Elektronik noter oluşturabilir ve bu noterden sertifikalar üretebilir.
- Güvenli sanal ağ kimlik doğrulamasında GizliKelime ve x509 sertifikaları olmak üzere iki ayrı yöntem desteklenmektedir.
- AES, DES, 3DES, BLOWFISH, CAST algoritmaları kullanılarak şifreleme yapılabilen ve MD5 ve SHA1-2 algoritmaları ile veri bütünlüğü sağlanabilmektedir.
- GSA bağı koptuğunda otomatik olarak tekrar bağlanmaya çalışır.
- IPSEC destekli bir çok sistemle çalışabilir.
- Donanımsal kripto kartları ile çok yüksek performanslara çıkabilir.



- Merkezin şubeleri ile internet üzerinden GSA bağlantısı

g) Kuyruk Yönetimi - Uygulama IP Trafiği Önceliklendirme

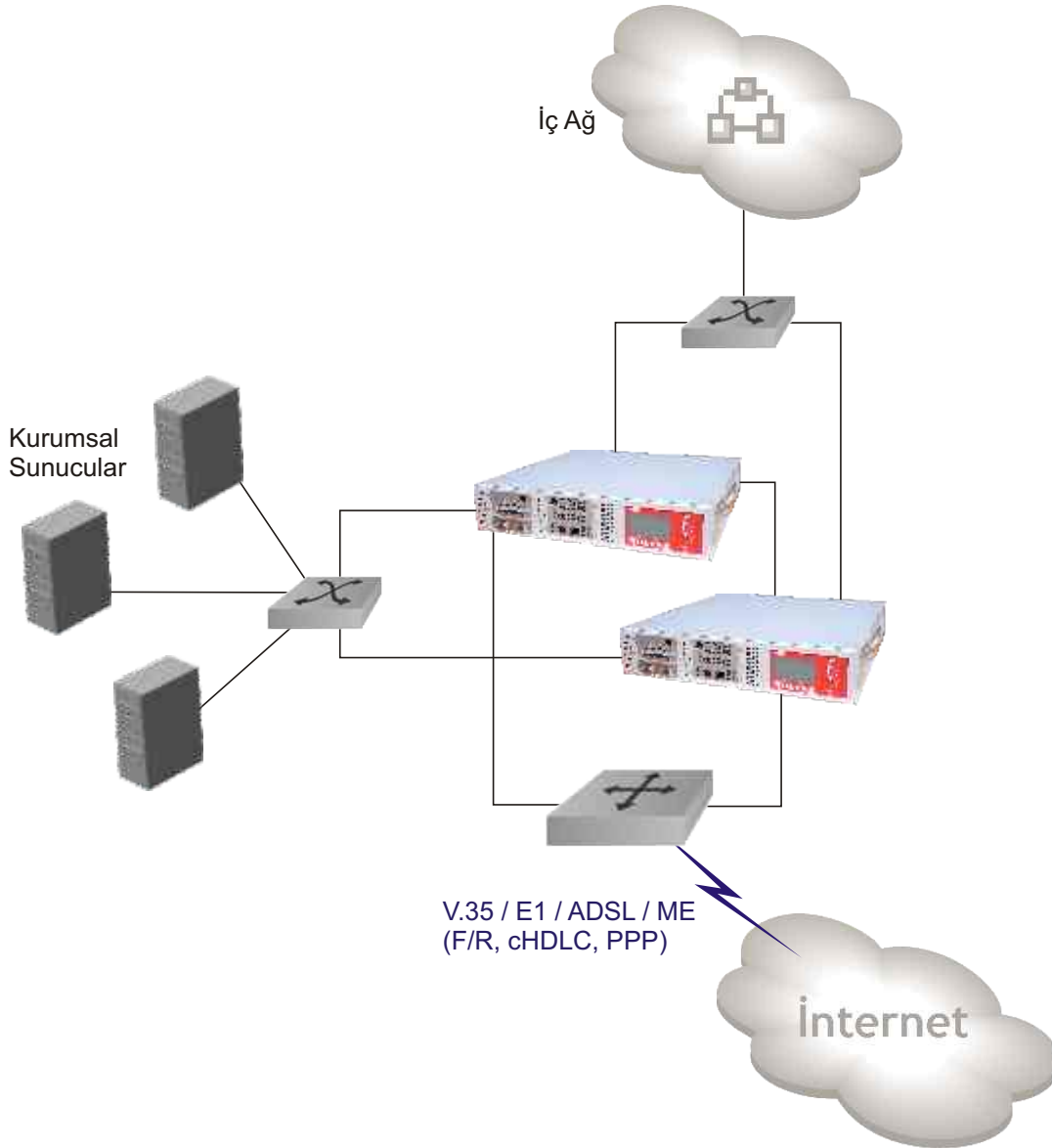
- i-bekçi üzerinden geçen, ses gibi kritik öneme sahip IP trafiğin önceliklendirilmesi sağlar.
- Kural bazlı trafik önceliklendirebilir.
- Öncelik derecesi veya dinamik sığa ayırımına göre önceliklendirme yapabilir.
- Kuyruk tıkanma uyarısı (ECE) yapabilir.



- Kurumsal kaynakları hat sığa yönetimi ile önceliklendirme

h) Küme

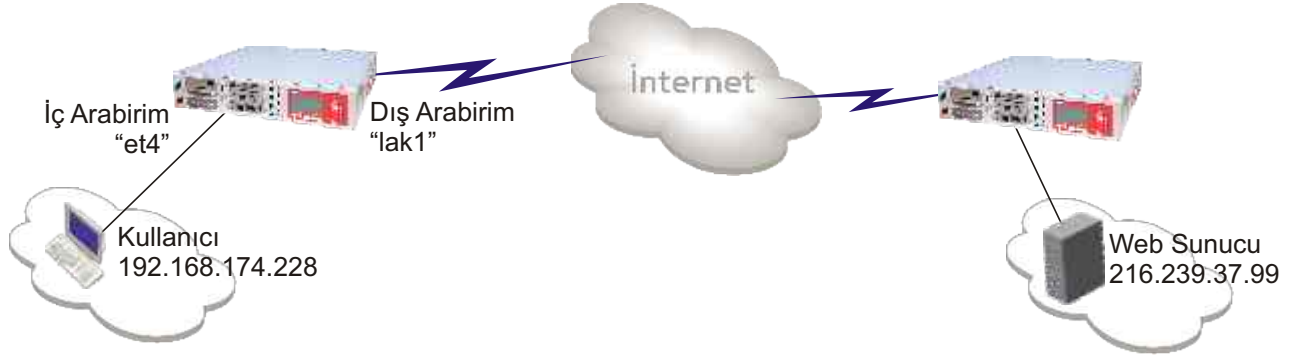
- Yüksek çalışabilirlik ve yedeklilik ya da sadece yapılandırma paylaşmak amacıyla iki i-bekçi arasında kümeleme işlemi yapılabilir.
- İki i-bekçi tek bir i-bekçi gibi çalışır. Etkin veya yedek i-bekçi üzerinde yapılan her türlü ayar ve yapılandırmalar her iki i-bekçi'de birden saydam olarak ele alınır, saklanır.
- Etkin i-bekçi devre dışı kaldığında diğer i-bekçi, trafik kaybettirmeden görevi üstlenir.
- Yük paylaşımı sağlar.
- Yedekli yapıda güncelleme ve bakım işlemleri, kesintisiz yapılabilir, böylece e-bilgi güvenliğinin sürekliliği sağlanır.
- IP durum ve Güvenli Sanal Ağ bilgileri eşgüdümленir.
- Etkin-Etkin veya Etkin-Yedek şeklinde çalışabilir.



- İki i-bekçi'nin yedekli çalışması

i) Trafik İzleme

- i-bekçi arabirimleri üzerinden geçen IP trafiğinin izlenmesini sağlar. Bu sayede i-bekçi üzerindeki IP tabanlı uygulamaların hatalarının bulunması, izlenmesi, yapıdan bağımsız olarak i-bekçi üzerinde yapılır.
- Arabirim bazlı olarak IP, kapı, iletişim kuralı vb. gibi ölçütlere göre trafiği ayrıştırıp izleme imkanı vererek iletişim hatalarının bulunmasını sağlar.
- Geçen paketlerin veri (ham) hallerini gösterebilir.



```

I-Bekçi Uçbirim Ekranı - v2.2.2
Dosya Düzenle Görünüm Araçlar Yardım

ss(##)/td lak1
tcpdump: listening on tun0, link-type LOOP
85.101.126.212.64260 > 212.58.226.19.80: P 1:581(580) ack 1 win 65535
66.249.93.104.80 > 85.101.126.212.56739: F 1:1(0) ack 1 win 8190
85.101.126.212.56739 > 66.249.93.104.80: . ack 2 win 65535
207.126.111.225.80 > 85.101.126.212.59697: . ack 464 win 1716 <nop,nop,timestamp 2458256777
1947036569> (DF)
212.58.226.19.80 > 85.101.126.212.64260: . ack 581 win 6960 (DF)
212.58.226.19.80 > 85.101.126.212.64260: . 1:1441(1440) ack 581 win 6960 (DF)
212.58.226.19.80 > 85.101.126.212.64260: . 1441:2881(1440) ack 581 win 6960 (DF)
85.101.126.212.64260 > 212.58.226.19.80: . ack 2881 win 65535
66.249.93.104.80 > 85.101.126.212.52599: F 1:1(0) ack 1 win 8190
85.101.126.212.52599 > 66.249.93.104.80: . ack 2 win 65535
66.249.93.104.80 > 85.101.126.212.60597: F 1:1(0) ack 1 win 8190
85.101.126.212.60597 > 66.249.93.104.80: . ack 2 win 65535

```

- td komutu ile dış arabirimdeki tüm trafiği izleme

```

I-Bekçi Uçbirim Ekranı - v2.2.2
Dosya Düzenle Görünüm Araçlar Yardım

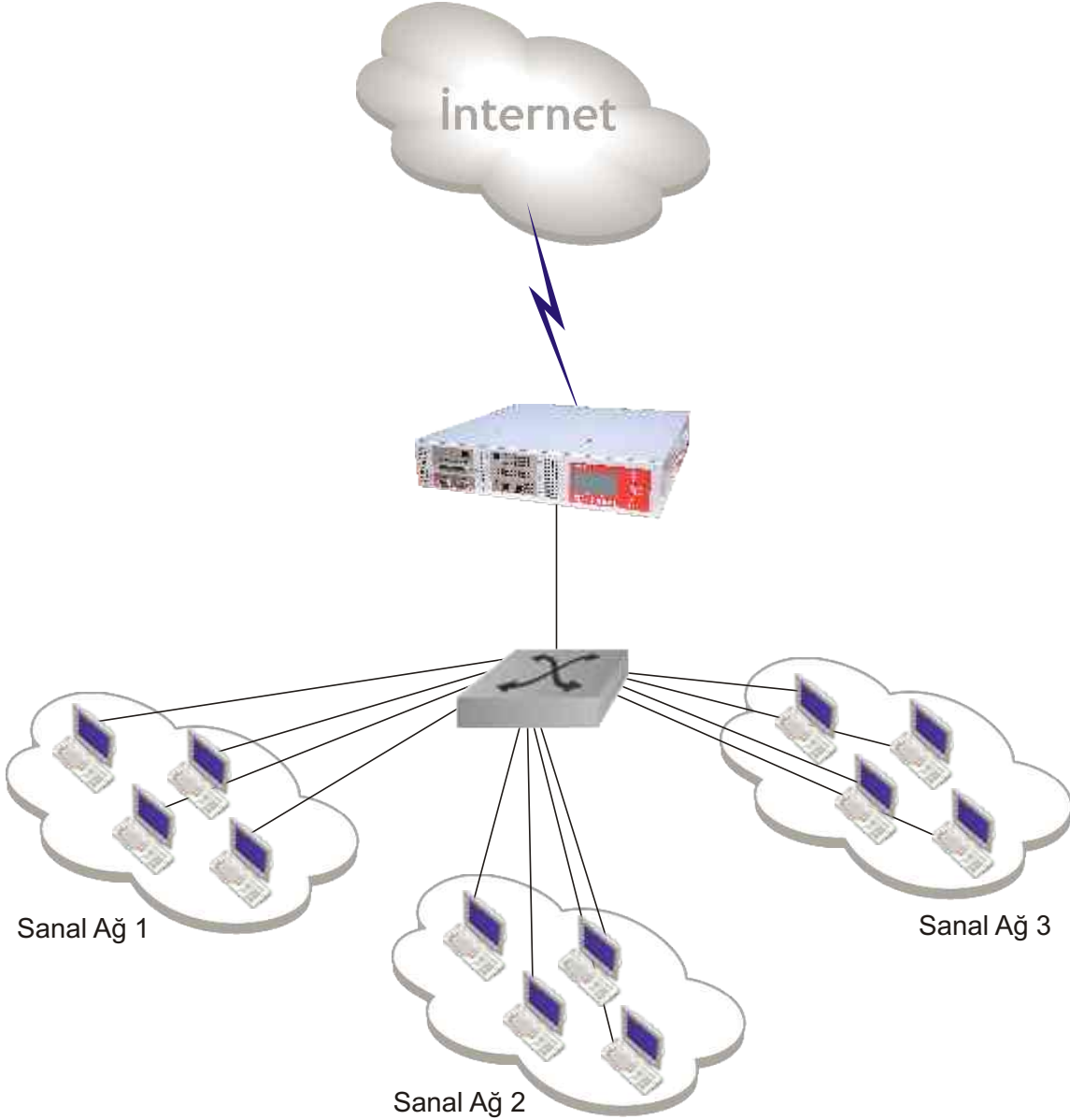
ss(##)/td et4 host 192.168.174.228 and port 80
tcpdump: listening on r10, link-type EN10MB
0:6:25:29:91:52 0:3:1d:2:49:b 0800 60: 192.168.174.228.1420 > 216.239.37.99.80: . ack 1 win 17280 (DF)
0:6:25:29:91:52 0:3:1d:2:49:b 0800 562: 192.168.174.228.1420 > 216.239.37.99.80: F 1:509(508) ack 1 win 17280
(DF)
0:3:1d:2:49:b 0:6:25:29:91:52 0800 60: 216.239.37.99.80 > 192.168.174.228.1420: . ack 509 win 7682
0:3:1d:2:49:b 0:6:25:29:91:52 0800 60: 216.239.37.99.80 > 192.168.174.228.1420: . ack 509 win 6432 [tos 0x10]
0:3:1d:2:49:b 0:6:25:29:91:52 0800 219: 216.239.37.99.80 > 192.168.174.228.1420: P 1431:1596(165) ack 509 win
6432 [tos 0x10]
0:3:1d:2:49:b 0:6:25:29:91:52 0600 1484: 216.239.37.99.80 > 192.168.174.228.1420: . 1:1431(1430) ack 509 win
6432 [tos 0x10]
0:6:25:29:91:52 0:3:1d:2:49:b 0800 60: 192.168.174.228.1420 > 216.239.37.99.80: . ack 1 win 17280 (DF)
0:6:25:29:91:52 0:3:1d:2:49:b 0800 60: 192.168.174.228.1420 > 216.239.37.99.80: . ack 1596 win 17280 (DF)

```

- td komutu ile iç arabirimde IP ve Kapı bazlı trafik izleme

j) Sanal Ağ, 802.1q

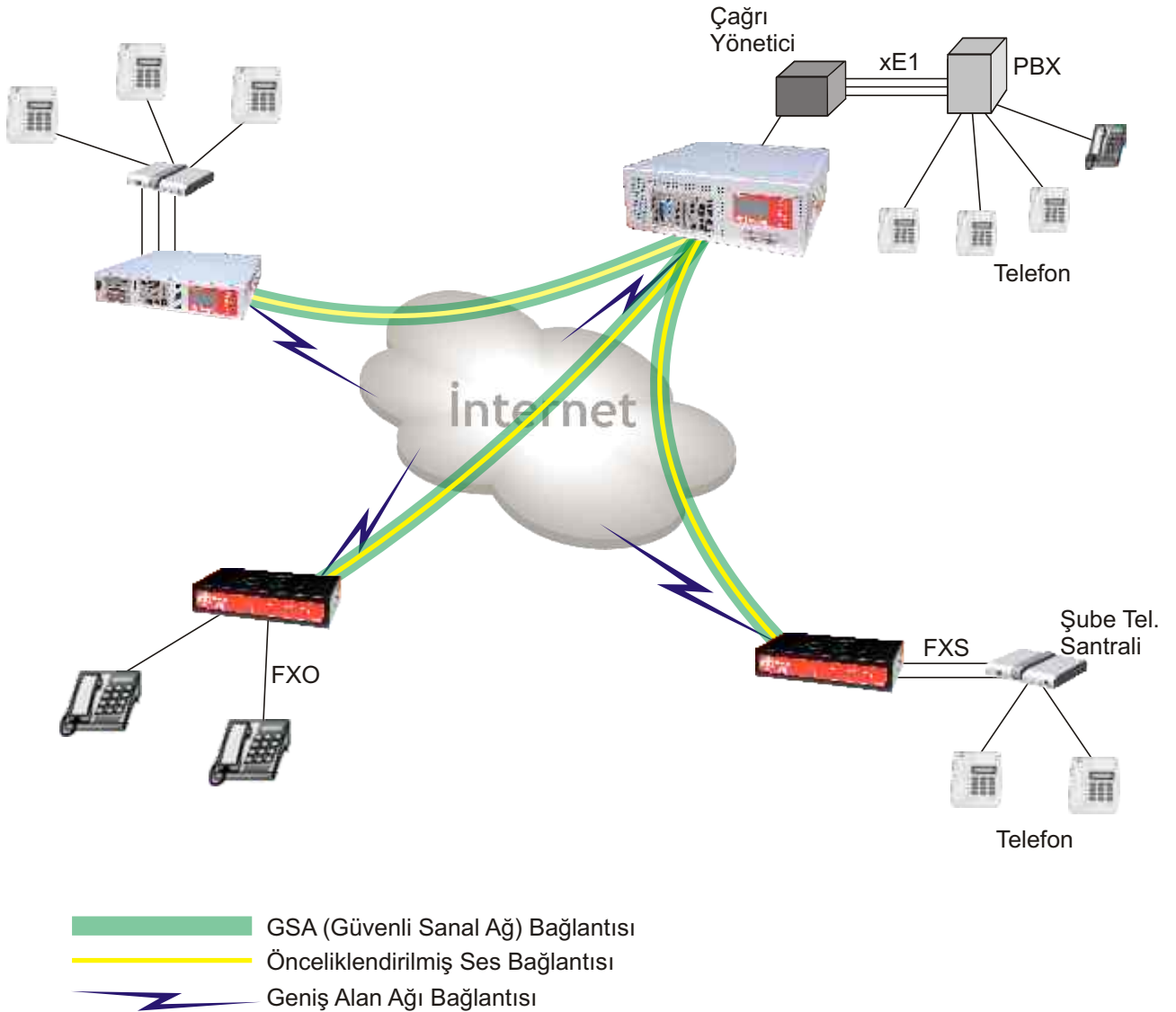
- Tek bir fiziksel arabirim üzerinden farklı ağlara üye olunmasını sağlar. Bu sanal ağ arabirimleri üzerinde kural yazılabilir, gerçek birer arabirim gibi kullanılabilir.
- i-bekçi, arkasındaki iç ağlarda kurulan sanal ağ yapılarının dış dünyaya olan bağlantılarını yönetebilir, denetleyebilir.



- i-bekçi ile sanal ağları internete bağlama

k) Ses İletişimi *

- FXS ve FXO arabirimleri sayesinde ses taşıyabilir.
- SIP/H.323 protokollerini destekler.
- IP üzerinden giden ses trafiğini önceliklendirebilir, kriptolayabilir.
- i-bekçi, ses trafiğini, Hacıyatmaz teknolojisi ile, son kullanıcıya saydam bir şekilde, farklı Geniş Alan Ağı arabirimleri arasında kriptolu olarak, önceliklendirebilir, yedekleyebilir.



*) 2006 ikinci yarısından sonra planlanan

a) Kural Üreteci

i-bekçi erişim denetiminin yapılandırıldığı arayüzdür. i-bekçi Paket eleği işlevselliğinin görsel olarak yönetilmesini sağlar. Sürükle bırak, çevrim içi yardım dosyaları, Türkçe dili ile kullanım kolaylığı sağlar. TCP/IP ve kullanıcı tabanlı olarak modelleme yapılabilir. Zamana bağlı olarak modellenen güvenlik politikalarının gerçekleştirilmesini sağlar.

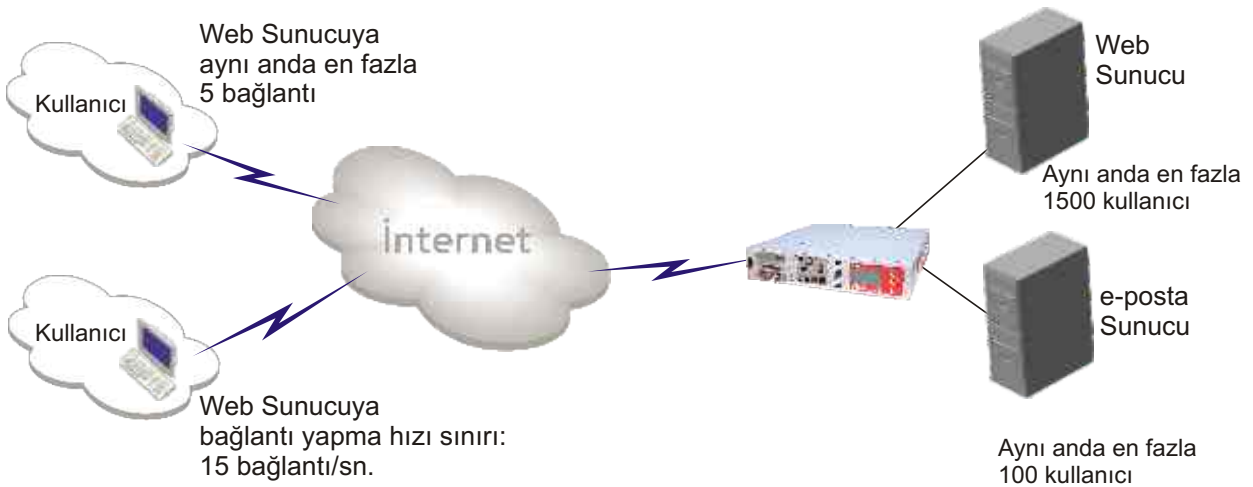
Adres Dönüşümü	Yöneltilme	Kullanıcı Yönetimi	Paket Eleği	Hedef	İletişim Kuralları	Kurullar	Özellikler	İşlem
Kayıtlı	Analiz			http, PtpVoice	tcp		Durum Kuru, Hemen, Günlük Tut	
Kayıtlı	Analiz			ssh			Durum Kuru, Hemen, Günlük Tut	şhdil...
Kayıtlı	Analiz			ps2-sistemcom			Durum Kuru, Hemen, Günlük Tut	şhdil...
Kayıtlı	Analiz						Durum Kuru, Hemen, Günlük Tut	şhdil...
Kayıtlı	Analiz						Durum Kuru, Hemen, Günlük Tut	şhdil...
Kayıtlı	Analiz				icmp, tcp, udp, esp		Durum Kuru, Hemen, Günlük Tut	
Kayıtlı	Analiz			zaptive, ssl	tcp		Günlük Tut, Durum Kuru, Hemen	şhdil...
Kayıtlı	Analiz			zaptive, ssl	tcp		Günlük Tut, Durum Kuru, Hemen	
Kayıtlı	Analiz			raportasadecek (6)	udp		Hemen	
Kayıtlı	Analiz						Günlük Tut	
Kayıtlı	Analiz						Günlük Tut	

- e-Bilgi güvenliği için kurumsal nesnelerin tanımlanmasını sağlar. (Ağ adresi, sunucu bilgisayar, kullanıcı, zaman vb. gibi)
- Kurumsal e-Bilgi güvenliği modellenebilir.
- i-bekçi güvenlik dilinin, şematik olarak yönetilmesini sağlar.
- i-bekçi ve kullanıcı bilgisayarı arasında güvenli (kriptolu) iletişim kurarak kuralları alır, hazırlanan kuralları i-bekçi'ye yollar.
- Active Directory, Ldap veya Radius'a bağlanıp kullanıcı listesini alıp, bunlar üzerine kural yazabilir.
- i-bekçi için Paket Eleği, Ağ Adres Dönüşümü ve Yöneltilme kuralları modellenebilir.
- Kural tabanlı olmak üzere;
 - Trafik önceliklendirme,
 - Uygulama seviyesinde yük dağıtımını ayarlama,
 - Birden fazla hattın yük dağılımı,
 - TCP bağlantı protokolü parametreleri,
 - Erişimi engellenen IP paketlerine uygun cevap metodu (ICMP cevabı dönmesi sağlanabilir/engellenebilir, TCP cevabı dönmesi sağlanabilir),
 - Günlük tutma
 ayarlarının yapılmasını sağlar.
- i-bekçi arabirimleri üzerinde sığa belirlemeye imkan verir.
- Paket yeniden düzenleme (assemble-reassemble) kabiliyeti vardır.
- Uygulanan kurullarla ilgili kayıt tutarak i-bekçi üzerinden geçen trafiğin, Raporlama Araçları aracılığıyla geçmişe yönelik incelenmesine imkan verir.
- Oluşturulan kurullar tekrar kullanılmak üzere saklanabilir arşiv amaçlı yedeklenebilir.
- i-bekçi, doğrudan ya da Kural Üreteci vasıtasıyla birçok servis reddi saldırılarına izoledir.

Servis Kalitesi Seçenekleri

Kurumsal servislere izin verilen bazı erişimler, kötü amaçla kullanıldığında servislerin hizmet sunmasını engelleyecek duruma getirebilir. Kurumsal hizmetlerin aksamaması için izin verilen IP erişimlerinin, iş süreçleri doğrultusunda modellenmesi i-bekçi Kural Üretici sayesinde mümkündür.

- Yazılan herhangi bir kuralın en fazla kaç istemci bilgisayara uygulanacağını belirleyerek, sunucu başına düşen bilgisayar erişimini kısıtlamış olur (Bilgisayar / Sunucu).
- Bir kuralla ilgili en fazla kaç durum oluşturulacağını belirleyerek muhtemel saldırıları engeller (Durum / Kural).
- Bir bilgisayardan en fazla kaç TCP bağlantısı yapılabileceği belirlenerek muhtemel saldırıları engellemesi sağlanır (Bağlantı / Bilgisayar).
- Bir bilgisayardan yapılacak TCP bağlantılarının sıklığı belirlenerek muhtemel saldırıları engellemesi sağlanır (Bağlantı / Saniye).
- Gelen paketlerin en fazla kaç parçaya ayrılabilceği belirlenerek muhtemel saldırıları engellemesi sağlanır.

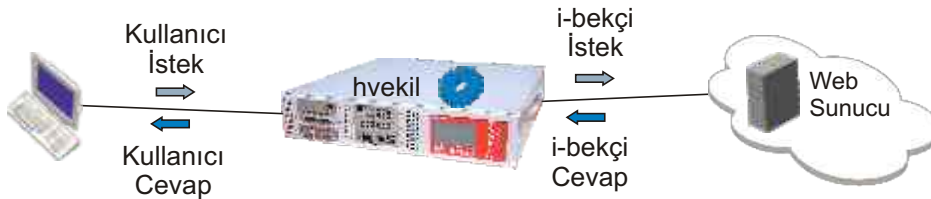
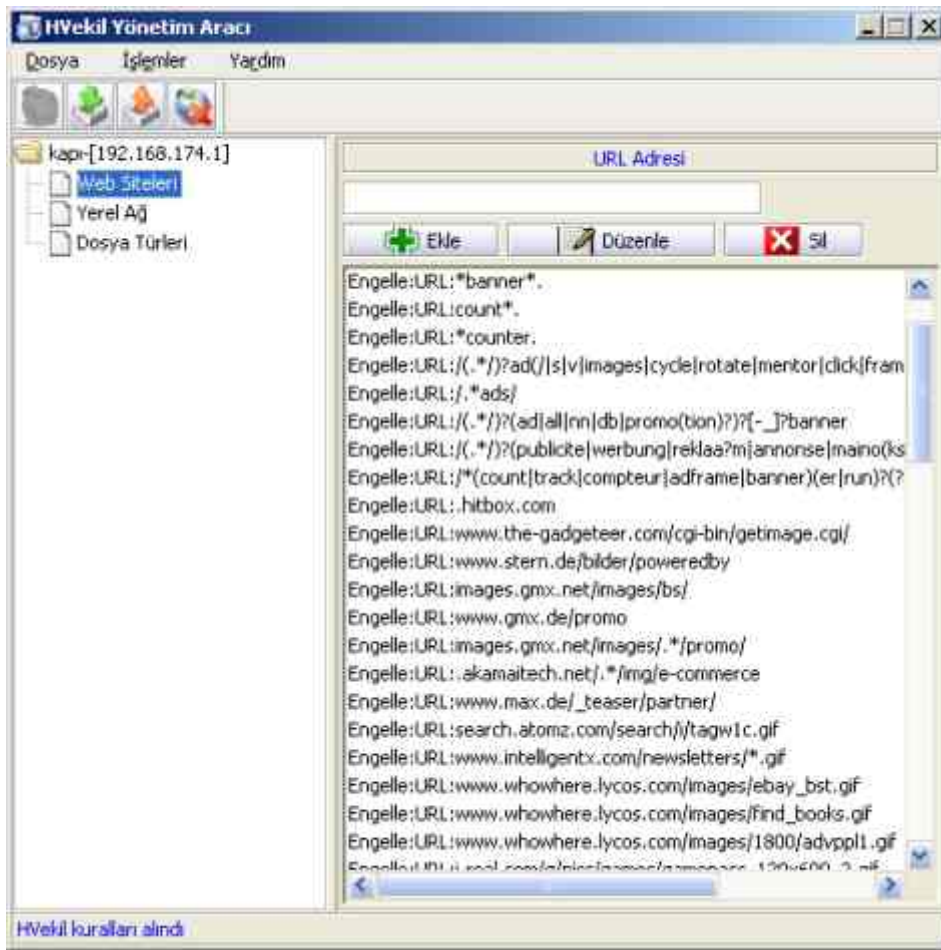


- Kural üretici ile servis kalitesi ayarları

b) Web Eleği *

i-bekçi koruduğu ağlarda bulunan istemci bilgisayarların yerine web bağlantılarını gerçekleştirebilir, bu sayede istemci bilgisayarların türleri, IP adresleri, web gezginleri gibi kişisel veya kurumsal bilgilerinin ortaya çıkması engellenmiş olur.

- http vekil sunucusuyla iletişim kurabilir.
- http vekil olarak çalışabilir ve Web Eleği ayarları HVEkil Yönetim Aracı'ndan yapılır:
- http istemlerine izin verilecek yerel ağdaki bilgisayarları belirler.
- Engellenmesi istenen MIME türleri belirlenebilir (uygulama, ses, görüntü vb. gibi).
- Engellenmesi istenen sitelerin tümünden alan adları veya alt adresleri veya türleri belirlenebilir.
- Engellenmesi istenen dosya uzantıları belirlenebilir (.mp3, .rar,... gibi).
- Web sitesi adresi, dosya türü yazımında joker karakterler (*,?) kullanılabilir.
- Belirlenecek kullanıcıları veya web sitelerini kurallardan muaf tutabilir.
- Engellenen URL adresine gitmek isteyen kullanıcıları izlemeye olanak verir.



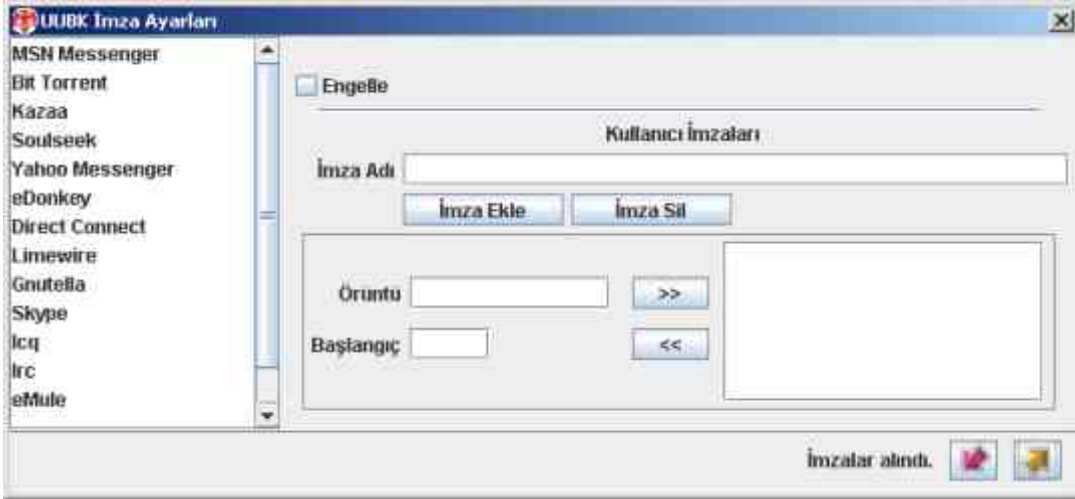
- hvekil'in çalışma mekanizması

*) 2006 ikinci yarısından sonra planlanan

c) İmza Yönetici / Paket İşleyici

İmza tabanlı olarak çalışan paket işleyici, i-bekçi üzerinden geçen tüm paketleri arabirim bazlı olarak dinler ve ilgili imza yakalanınca bunu i-bekçi Saldırı Önleme Sistemi'ne (SÖS) verir, Saldırı Önleme Sistemi bu bağlantının durumlarını kopartır ve hedef IP adresin erişimini keser. Uçtan uca bağlantı imzaları i-bekçi içinde öntanımlı olarak bulunur. İstenilen tüm imzaların, iletişim içinde aranabilmesi mümkündür.

- IP paketleri üzerinde işlem yapmak üzere tasarlanmış ve iki IP arasında uçtan uca kurulmuş olan bağlantıları imza tabanlı olarak inceleyip, gerekirse bağlantıları kesme yetisine sahip bir mekanizmadır.
- i-bekçi üzerinde arabirim bazlı çalışır.
- Arabirim üzerinden geçen IP paketlerinin yüküne bakarak düzenli veya düzensiz olarak ifade edilebilen imzaları/örüntüleri bulur.
- Uçtan uca bağlantı kesici olarak çalıştırılan paket işleyici, ön tanımlı olarak bilinen uçtan uca bağlantı iletişimini kesmek için yapılandırılmıştır.
- i-bekçi yöneticileri IP paketleri içindeki istedikleri herhangi bir örüntüyü buldurup durdurabilirler.



- Uçtan uca kurulmaya çalışılan bağlantıların kesilmesi

Erişim Gösterici

- Erişim Gösterici, yerel bilgisayarın uzaktaki bilgisayara olan, i-bekçi kurallarına göre izin verilen ya da verilmeyen erişimleri gösterir.
- Erişim Göstericiye gelen tüm erişim bilgileri arasından, verileri, Kaynak IP, Kaynak Kapı, Hedef IP, Hedef Kapı, Arabirim, paketlerin, Yön ve İzin bilgilerine göre ayıklayarak, kullanıcıya sadece istenen bilgiyi gösterir.
- Azami erişim sayısı belirlenerek, tabloda süzme işlemine tabi tutulmuş erişimlerin izlenmesi ölçeklendirilmiş olur.
- O an tablodaki erişimler arasında arama yaparak, aranan verinin geçtiği erişimleri gösterir.

Zaman	Kaynak IP	Kaynak Kapı	Arabirim	Yön	Hedef IP	Hedef Kapı	İzin	İletişim Kurallı	Kural No	Sebep	İşaretle
13:34:41	192.168.174.18	1108	et4	İçeri	193.140.238.6	53 / domain	Geçti	UDP	33(132)	Kuralla uydu	
13:34:41	192.168.174.18	1109	et4	İçeri	205.188.229.57	80 / http	Geçti	TCP	10(43)	Kuralla uydu	S
13:34:38	192.168.174.92	1503	et4	İçeri	208.191.52.50	80 / http	Geçti	TCP	10(43)	Kuralla uydu	S
13:34:45	192.168.174.151	54045	et4	İçeri	89.151.208.245	33627	Geçti	UDP	33(132)	Kuralla uydu	
13:34:59	192.168.174.228	1288	et4	İçeri	24.176.168.4	1080	Takıldı	TCP	11(44)	Kuralla uydu	S
13:34:59	192.168.174.228	40242	et4	İçeri	24.176.168.4	58397	Geçti	UDP	33(132)	Kuralla uydu	

Erişim Sayısı: 25 Veri alındı: 13:35:03

Zaman	Kaynak IP	Kaynak K.	Arabirim	Yön	Hedef IP	Hedef	İzin	İletişim	Kural	Sebep	İş...
11:40:40	85.97.109.100	59065	lak2	Dışarı	195.175.37.14	53 / d...	Geçti	UDP	20(1...	Kuralla uydu	
11:40:45	192.168.174.112	54045	et4	İçeri	81.13.227.148	24353	Geçti	UDP	33(1...	Kuralla uydu	
11:40:46	85.97.109.100	59065	lak2	Dışarı	81.13.227.148	24353	Geçti	UDP	33(1...	Kuralla uydu	

Günlük Gösterici

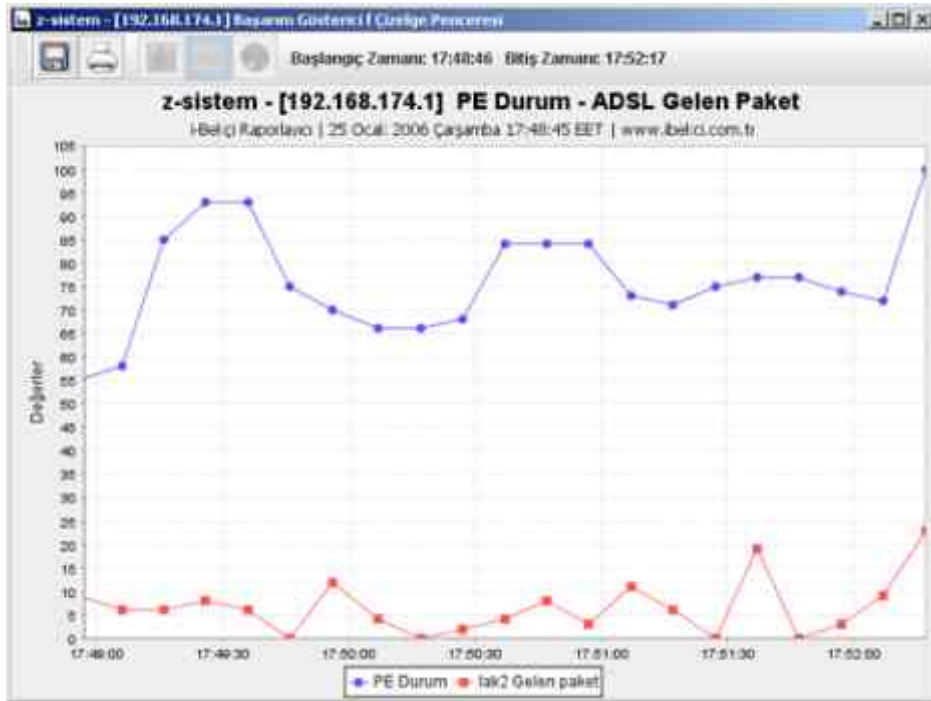
- Günlük Gösterici i-bekci'nin ürettiği günlük bilgilerini gösterir.
- Günlük bilgileri, bütün olarak ya da günlük verisini oluşturan alt-sisteme göre sınıflandırılarak gösterilebilir.

Zaman	Kaynak	Mesaj
13:44:21	ppp	tun0: Chat: deflink: Redial timer expired.
19:27:07	ppp	tun0: Chat: deflink: Redial timer expired.
19:27:07	iBekci	zs: 7: Ayarlar saklandı: 192.168.174.228 1960 22
19:27:07	/bsd	real mem = 131899392 (128808K)
19:27:07	/bsd	cpu0: FPU,V86,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,M...
19:27:07	/bsd	cpu0: Intel(R) Celeron(R) CPU 2.40GHz ("GenuineIntel" 686-class) 2.40 ...
19:27:07	/bsd	root@ibc38: /sys/arch/i386/compile/d5
19:27:07	/bsd	OpenBSD 3.8-stable (d5) #5: Sat Nov 19 16: 46: 30 EET 2005
19:27:07	syslogd	restart
19:27:07	syslogd	exiting on signal 15
19:27:07	reboot	rebooted by root
19:26:03	ntpd	listening on 192.168.10.2
19:26:03	ntpd	ntp engine ready
19:21:40	ntpd	listening on 192.168.8.2
19:21:40	ppp	tun0: Chat: deflink: Reconnect try 6071 of 0
19:21:40	ppp	tun0: Chat: deflink: Reconnect try 6070 of 0
19:21:40	sshd	Invalid user deneme from 192.168.174.228
19:21:40	sshd	Failed password for invalid user deneme from 192.168.174.228 port 1957 ...
19:21:40	sshd	Failed none for invalid user deneme from 192.168.174.228 port 1957 ssh2
19:21:40	sshd	Failed none for ibekci from 192.168.174.228 port 1960 ssh2
13:46:14	sshd	Accepted password for ibekci from 192.168.174.228 port 1960 ssh2

Rapor Sayısı: 500 Veri alındı: 13:55:15

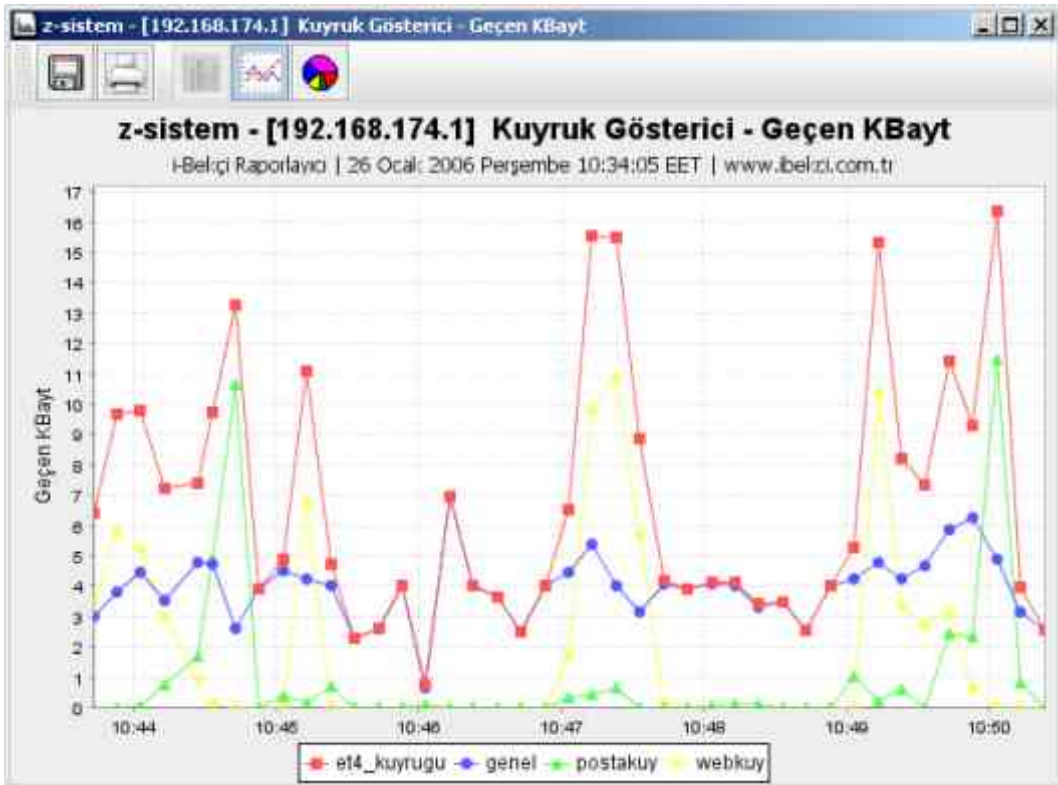
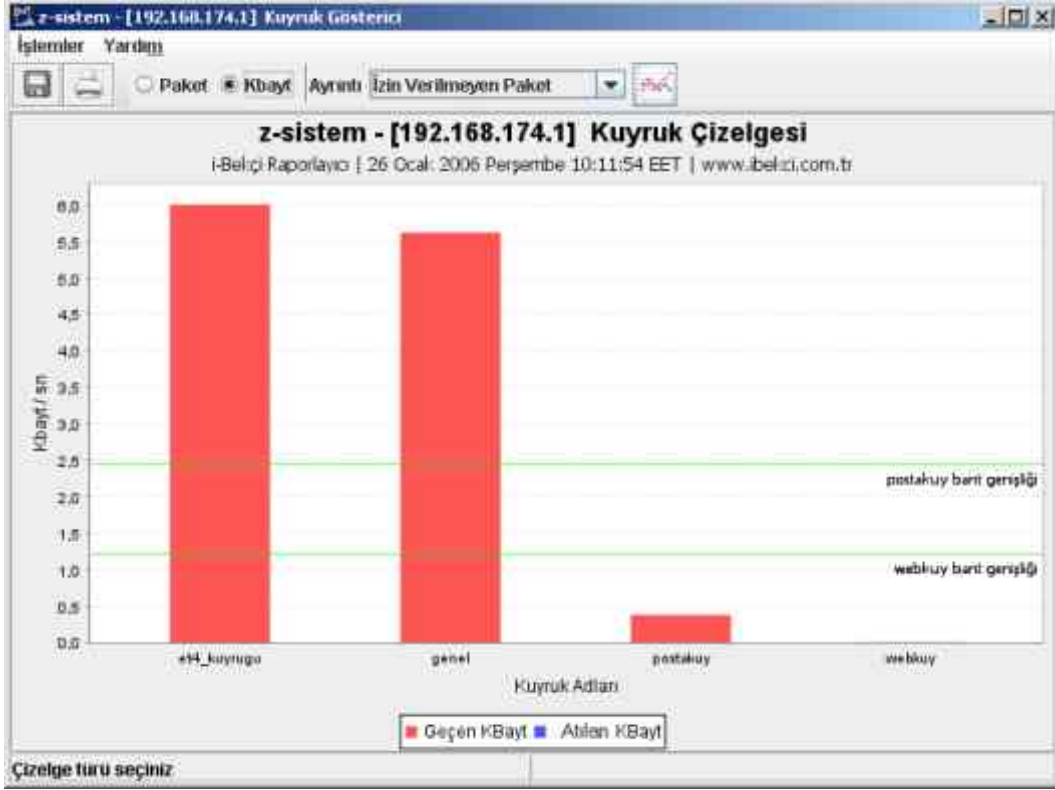
Başarım Gösterici

- i-bekçi'nin başarım verisi ile Merkezi İşlem Birimi, Bellek, Paket Eleği ve Arabirimler incelenebilir.
- i-bekçi yöneticileri, bu başarım verilerini topluca ya da ayrı ayrı izleyebilir.
- Başarım verileri sayısal ya da yüzde olarak ifade edilebilir.
- Başarım niteliklerinden seçilenleri çizelge halinde gösterir. İstendiğinde var olan çizelgeye ekleme ya da çıkarma yapılabilir.
- Kullanıcıya kolaylık açısından gösterilmiş olan çizelgelerin adı ve nitelikleri yeniden kullanım için saklanır.



Kuyruk Gösterici

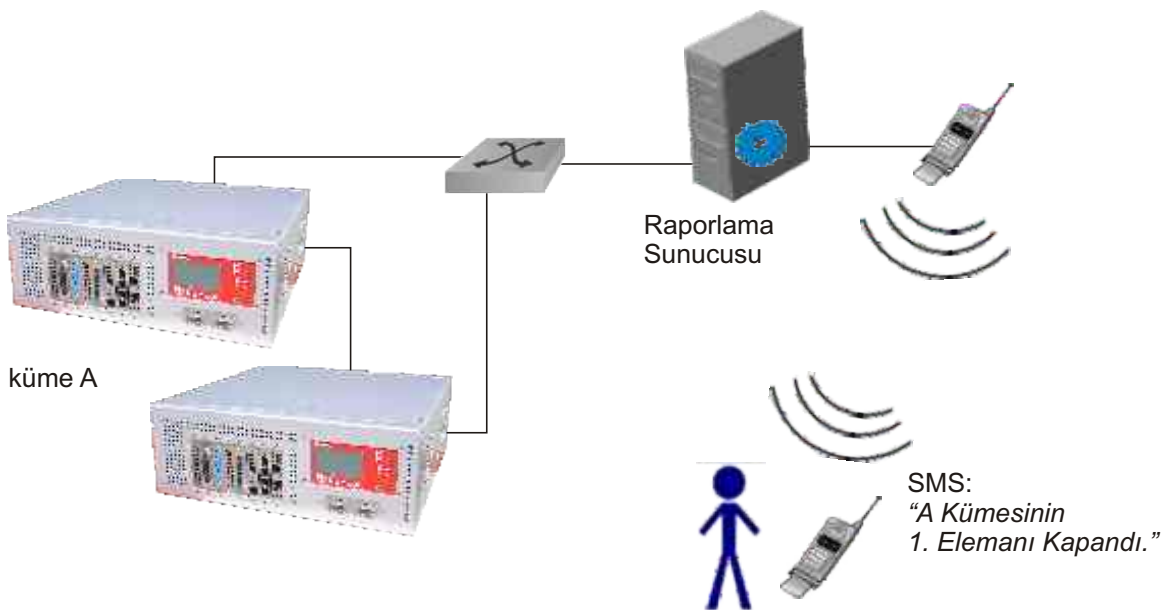
- Kuyruk Gösterici, i-bekçi'nin üzerindeki arabirimlerin kısıtlanmış kuşak genişliğinin hizmetlere göre bölünmesi sonucu oluşan kuyrukları grafiklerle gösterir.
- Grafikleri, Geçen Paket/Kbayt, İzin Verilen/Verilmeyen Paket/Kbayt ve kuyrukta bekleyen veya atılan paket sayısına göre çizdirmek mümkündür.



Uyarı Gösterici

- Uyarı Gösterici, Durum, Erişim, Günlük ve Başarım verilerini ele alarak uyarı bilgisi üretir ve oluşan uyarıları i-bekçi yöneticisine sunar.
- Üretilen uyarılar için e-posta atabilir.
- Üretilen uyarı için girilen bir numaraya faks çekilebilir. Bu özellik için, Raporlama Araçlarının çalıştığı bilgisayarda tanımlı bir faks-modem kartı olması ve telefon hattına bağlı olması gerekir.
- Her üretilen uyarı için girilen telefon numarasına SMS atılabilir. Bunun için bir cep telefonunun raporlama araçlarının çalıştığı bilgisayara bağlı olması ve ilgili sürücülerin yüklenmesi gereklidir. Not: Bu özellik için sadece Nokia marka cep telefonları desteklenmektedir.
- Her uyarı anlamsal olarak gruplandırılabilir ve bu gruplar, izlemenin kolay olması açısından ayrı gösterilebilir.

Uyarı Adı	Yıl	Müh	Saf	Kır	M. Değer	S. Değer	K. Değer	Zaman Aralığı	Zaman Aralığı
Hatalı Erişim	0	0	0	1	-1	-1	1	60	60
Kullanıcı Kabul	0	0	0	1	-1	-1	-1	-1	-1
EŞ Dosya Silindi	0	0	0	1	10	-1	60	60	60
Bekli Durum Değişliği	0	0	0	1	-1	-1	-1	-1	-1
Küme Düşüm Durumu	0	0	0	1	-1	-1	-1	-1	-1
Küme Düşüm Başlamıyca	0	0	0	1	1	-1	30	60	60
MBB	0	0	0	50	75	-1	-1	60	60
Bellek	0	47	0	30	50	-1	-1	60	60
Arabirisi Kullanım	0	0	0	10	30	-1	-1	60	60
PE Durum Artış	0	0	0	500	1000	-1	-1	60	60
Kullanıcı Gelen Veri	0	0	0	100	-1	-1	-1	60	60
Kullanıcı Gelen Veri	0	0	0	-1	-1	-1	-1	60	60
Telferi Erişim	0	5	0	10	50	-1	-1	60	60
Tek Kapıdan Servis Tarama	0	4	0	-1	5	-1	-1	60	60
Tek Kapıdan Tel Servis Tarama	0	1	0	1	5	-1	-1	60	60
Servis Tarama	0	7	0	1	5	-1	-1	60	60
Ağda Servis Tarama	0	26	0	10	50	-1	-1	60	60
Ağda Tel Servis Tarama	0	3	0	10	50	-1	-1	60	60
Tarih Değişliği	0	0	0	-1	-1	-1	-1	-1	-1
PE Kurul Yükleme	0	0	0	1	-1	-1	-1	-1	-1
İmza Yükleme	0	0	0	1	-1	-1	-1	-1	-1
Ayar Silinme	0	0	0	1	-1	-1	-1	-1	-1



- Uyarı Gösterici ile i-bekçi yöneticisine SMS gönderimi

Veritabanı Göstericiler

- Veritabanı (VT) Göstericiler, Başarım, Erişim, Durum, Günlük, Uyarı verisi ve Kuyruk verilerinin VT kaydediciler tarafından kaydedilen kayıtların, geçmişe yönelik olarak sorgulanmasını sağlar.
- i-bekçi yöneticisine seçenekler sunarak ya da sorgu için girdiler alarak, bu verilerin veritabanındaki sonuçlarını, tablolar ya da grafikler halinde sunar.
- Veritabanındaki kayıtlar, anlık veri gösterici bileşenlerine gelen verilerin sistematik olarak yapılan kayıtlarıdır.
- Erişim kayıtları çok fazla olabileceği için, kayıpsız olarak özetleme ile veri tabanına saklanır. (bir IP adresinden gelen ve kesilen IP paketleri bir kayıt olarak ele alınır)

Bağlantı Yönetici (BY)

- i-bekçi'den gelen başarım, paket eleği, oturum, erişim izni, günlük bilgilerini yastıklar ve dağıtımını yapar. Yastıklanan bilgileri biçimlendirerek, ilgili kaydediciye ve Raporlama Araçları programının ilgili göstericisine gönderir.
- Başarım, erişim, durum ve günlük kaydedici programlarından gelen uyarıları yastıklar. Yastıklanan bilgileri Raporlama Araçları programının Uyarı Gösterici bölümüne gönderir.
- i-bekçi'den gelen kuyruk bilgilerini yastıklar. Yastıklanan bilgileri biçimlendirerek, Raporlama Araçları programının Kuyruk Gösterici bölümüne gönderir.

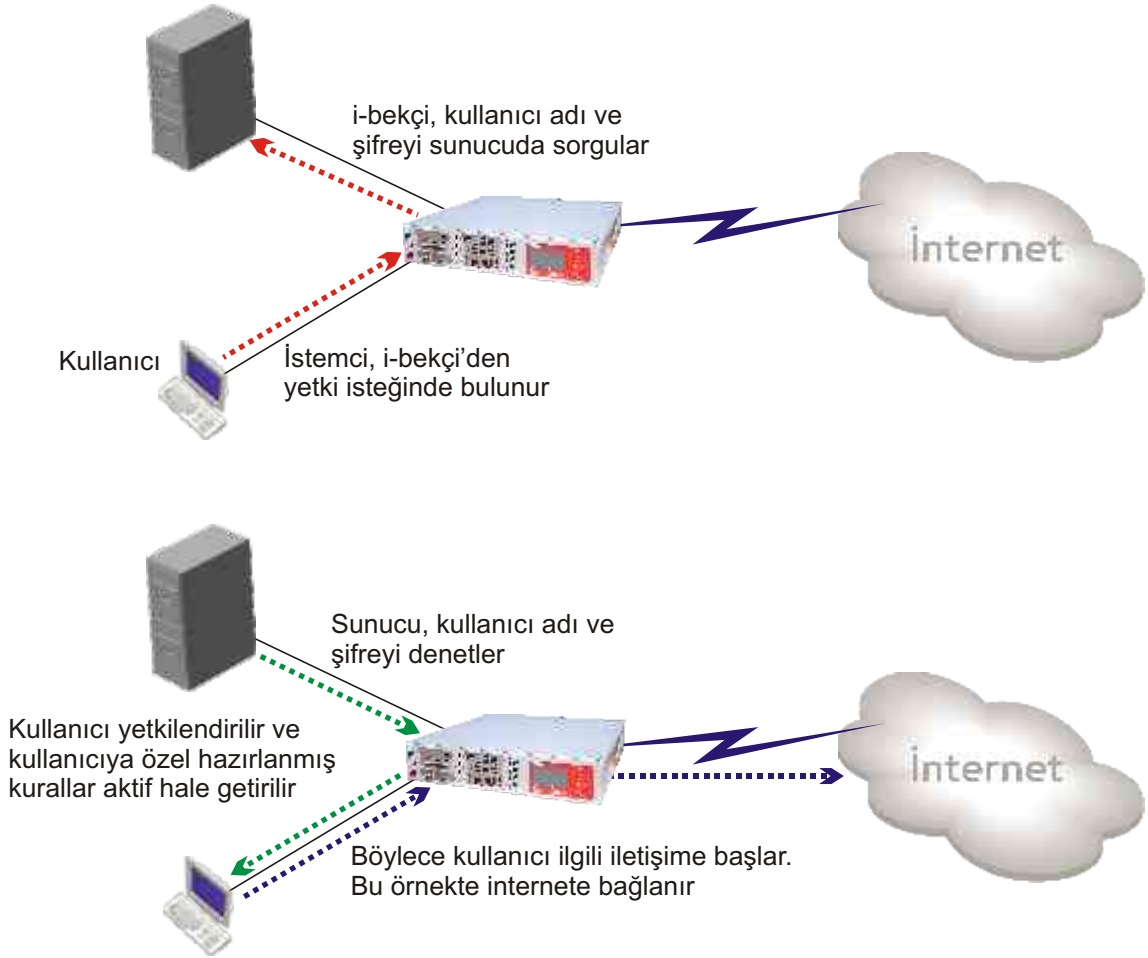
Veritabanı Kaydediciler

- ◆ Durum Kaydedici :
 - i-bekçi üzerinden geçmesine izin verilen bağlantıların oturum bilgilerinin veri tabanına kaydedilmesini sağlar.
 - Ağdaki kullanıcılardan aldığı ya da gönderdiği veri miktarı, belli bir seviyeyi aşanların bilgilerini bağlantı yöneticiye onun da vasıtasıyla Raporlama Araçları programının Uyarı Gösterici bölümüne gönderir.
- ◆ Erişim Kaydedici :
 - i-bekçi üzerinden geçmesine izin verilen ve verilmeyen paketlerin bilgilerini Kaynak IP, Hedef IP, Hedef Kapı, İletişim Kuralı, Yönü ve geçip geçmediği bilgilerine göre özetleyerek veri tabanına kaydeder.
 - Saldırı teşkil etme olasılığı olan erişimler, Raporlama Araçları programının Uyarı Gösterici bölümüne gönderilir.
- ◆ Günlük Kaydedici :
 - i-bekçi günlük bilgilerini yorumlayarak veri tabanına kaydeder.
- ◆ Başarım Kaydedici :
 - i-bekçi'den gelen başarım bilgilerini veri tabanına kaydeder.
 - i-bekçi arabirimlerinden gelen giden paket sayısı, ana bellek kullanımı ya da merkezi işlem birimi kullanımı belli bir değeri geçtikten sonra uyarı üretilir. Uyarı bilgisi, bağlantı yöneticiye, onun vasıtasıyla da Raporlama Araçları programının Uyarı Gösterici bölümüne gönderilir.
- ◆ Kuyruk Kaydedici :
 - i-bekçi üzerinde tanımlı olan kuyrukların bilgileri Paket Eleğinden gelir.
 - Kuyruk Kaydedici, Bağlantı Yönetici'den aldığı kuyruk bilgilerini veritabanına kaydeder.
 - Kuyruk bilgileri, izin verilen ya da verilmeyen tüm trafiğin istatistiklerini içerir.
- ◆ Uyarı Kaydedici :
 - Diğer tüm kaydedicilerin oluşturdukları ve gönderdikleri uyarı bilgilerini Bağlantı Yönetici'den alıp, veritabanına kaydeder.
 - Bağlantı Yönetici'den aldığı uyarıları Uyarı Gösterici'ye aktararak hizmet verir.

e) Kullanıcı Yönetimi

iDi (i-bekçi Dizin İstemcisi)

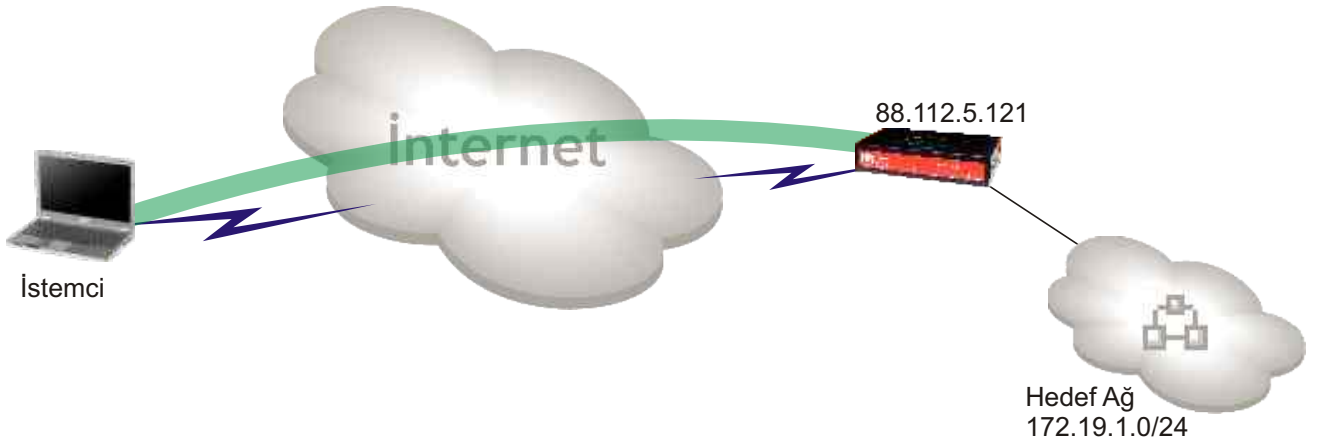
- i-bekçi ile güvenli bağlantı kurarak, kullanıcının Active Directory, Ldap ya da Radius yetkilendirmesinin yapılmasını sağlar. Windows işletim sistemi için geliştirilmiştir.
- Yetkilendirme sonrasında i-bekçi'ye bağlı kaldığı sürece, İDİ çalıştıran kullanıcının, kendisine veya grubuna özgü yüklenmiş kurallar ile i-bekçi üzerinden erişim yapmasını sağlar.
- Etkinlik alanı içinde i-bekçi yöneticisi tarafından belirlenmiş ayarları kullanır.
- İDİ, kullanıcı adını ve şifresini saklayabilir.
- Kullanıcı adını Windows ortamından alabilir.
- Bağlantı koptuğunda i-bekçi'ye otomatik olarak tekrar bağlanmaya çalışır.
- İDİ durdurulduğunda ya da kapatıldığında kullanıcıya özel olarak uygulanmış kurallar hemen yürürlükten kaldırılır.
- Kurumsal ihtiyaçlar doğrultusunda yetkilendirme kriterleri genişletilebilir. (USB bellek kullanımı, bilgisayar üzerindeki ayırt edici bir bileşen numarası gibi ...)



- Kullanıcı yetkilendirme süreci

4. GSA İstemci

- Kullanıcının bilgisayarındaki Windows işletim sisteminden i-bekçi'ye Güvenli Sanal Ağ kurmasını sağlar.
- Gizli kelime veya X.509 sertifikaları ile Güvenli Sanal Ağ kurabilir.
- Windows tarafından sağlanan IPSEC yapılandırmasını kullanır.



- İstemci GSA uygulaması

Z-Sistem

2002 yılında, Bilgi İletişimi ve Güvenliği teknolojileri sektöründe ilk Türk BİG cihazı olan i-bekçi ile hizmet vermeye başlayan Z-Sistem, birçok kamu kuruluşu ve özel şirkete stratejik çözümler sunmaktadır. Birçok teknolojiyi tek bir potada toplamayı başaran Z-Sistem, Sanayi, İnşaat, Güvenlik, e-devlet, Medikal, Enerji ve Eğitim sektörlerine yıllardır i-bekçi üretmektedir. Müşteri odaklı AR-GE çalışmalarına önem veren Z-Sistem, i-bekçi ürün ailesini sürekli geliştirmektedir.



Uzmanlar Takımı



Z-Sistem ekibi, Bilgi İletişimi ve Güvenliği konusunda bilgi üreten, kendini sürekli geliştiren, inisiyatif kullanabilen, tecrübeli bir uzman mühendis ekibinden oluşmaktadır. Hızlı, güvenilir ve etkin hizmet sağlayan sürekli destek birimimiz, müşteri memnuniyetini en üst seviyede tutmayı hedeflemektedir. Z-Sistem destek takımı, danışmanlıktan, kuruluş ve eğitime, bakım ve onarımdan, güncelleme taleplerine kadar bir çok alanda çözüm ortakları ile beraber başarıyla faaliyet göstermektedir.

Bilgi İletişimi ve Güvenliğinde i-bekçi

Uzun bir ar-ge sürecinden sonra ulusal pazara sürülen i-bekçi, kısa zamanda e-devlet, finans, eğitim, internet servis sağlayıcılar, güvenlik ve özel sektör alanlarında bir çok projede aktif olarak rol almıştır. Z-Sistem ve i-bekçi, her an ulaşabileceğiniz üretici firma, değişen güvenlik ihtiyaçlarına yön veren uzman bir takım, ana dilinizde kolayca anlayıp kullanabileceğiniz yazılımlar, işlevsellik ve başarımlı iddiası, uygun fiyat politikası ve müşteriye dost yaklaşımıyla farklı bir anlayış sunmaktadır.



z-sistem

İnternet Servisleri, Bilişim Teknolojileri, Veri Güvenliği San. ve Tic. Ltd. Şti.

Tel : +90 312 238 2415 Faks : +90 312 238 2418
www.z-sistem.com www.i-bekci.com
bilgi@z-sistem.com

MERKEZ
Beyler Caddesi Dost Kent Yanı No:4
Çayyolu / ANKARA, TR, 06530

AR-GE
Hacettepe Üniversitesi Teknokenti
Beytepe / ANKARA, TR, 06532