

# Sanal IPv6 Balküpü Ağı Altyapısı: “KOVAN”



Yavuz Gökırmak, Onur Bektaş, Murat Soysal, Serdar Yiğit



- Balküpü, Balküpü ağı, Kovan öncesi
- Kovan gelişim aşamaları
- Yeni fırsatlar / yeni problemler
- Kovan bileşenleri
- Kovan nasıl çalışıyor ?
- Kovan yetenekleri
- Performans
- Sorular



- Balküpleri, ađ ve bilgi güvenliğine yapılan saldırıların farkına varmak, saldırganların yöntemlerini izlemek, metotlarını belirlemek ve yeni geliştirilen saldırı çeşitlerinden önceden haberdar olmak amacı ile dizayn edilmiş yazılım veya sistemlerdir
- Balküpleri üzerinde çalışan uygulamalar bilgisayar ve ađ üzerinden verilen servisleri öyküleyerek saldırganlara gerçek sistemler ile uğraştıkları izlenimini verir
- Balküplerinin amacı saldırıya uğramak ve kırılmaktır
- Bu görevi üstlenmiş makineler geçerli hiçbir servis sunmadıklarından, kendilerine yönlenen her türlü trafik şüpheli olarak kabul edilmekte ve inceleme altına alınmaktadır
- Balküpleri hali hazırda bilinen açıklar karşısında zayıf görünerek, bunları değerlendirmeye çalışan saldırganların tespitinde yardımcı olurlar
- Balküprü ađı balküplerinin bir araya gelerek oluşturdukları ađdır



- ULAKNET CSIRT Balküpü Çalışma Grubu
- 4 Seneden fazla bir süredir çalışan aktif IPv4 balküpü uygulaması
  - <http://istatistik.ulakbim.gov.tr/balkupu/>
- Balküpü İstatistikleri Servisi
- Balküpü & OLTA entegrasyonu
- AB 2007, AB 2008 Çalışma Grubu sunumları
- I.ULAKNET Eğitim ve Çalıştayı "Balküpü Test Yatağı Sunumu"
- I.ULAKNET Eğitim ve Çalıştayı "Honeyd Kurulumu Sunumu"
- II.ULAKNET Eğitim ve Çalıştayı "ULAKNET Balküpü Sistemi Sunumu"
- Ulak-CSIRT "Honeyd Kurulumu Belgesi"
- Ulak-CSIRT "Honeywall Kurulumu Belgesi"
- Soysal,M., Bektas O., Analysis of Attacks Towards Turkish Academic Network, ISCTURKEY'08, pp. 126-131, 25-27 December 2008, Ankara, Turkey



- **Balküpü Proje önerisi (2008)**
  - Sanal Servisler
  - Tek bir fiziksel sunucu üzerinde çalışan tek bir işletim sistemi
  - Geniş alan ağı
  - 2 Sunucusu (Balküpü ve önüne koyulacak monitör ve güvenlik cihazı)
  - Dünya hangi yöne gidiyor ? Sanallaştırma + Bulut bilişim..
- **Yeni Balküpü**
  - Sanal / gerçek servisler
  - Sanal makine (virtual machine)
  - Geniş Alan Ağı / Yerel Alan Ağı
  - 1 Sunucu
- **Peki ya ağı da sanallaştırırsak ?**
  - Sanal ağ
  - Sanal yönlendirici
  - Sanal anahtarlama cihazı



# Yeni Fırsatlar Yeni Problemleri Beraberinde Getirir

- Bağlantı tanımlanması, sanal servis, cihaz tanımlanması, sanal topoloji oluşturulması nasıl olacak ?
- Ağ trafiğinin izlenmesi ve günlüklerin takibi (netflow, SNMP vb)
- Sanal ağda yönlendirme protokolleri çalıştırılması (RIP, RIPng)
- Sanal ağ cihazlarını yönetimi nasıl olacak ?
- Performans ?
- Tüm bunları yönetecek yönetim arayüzü ?
- Oluşturulan sanal ağ/servis/günlük bilgileri nasıl kaydedilecek ?



- FreeBSD 8.1 işletim sistemi üzerinde geliştirildi
  - Kaynak kodundan derlenebileceği kurulum için hazır sanal makine imajları da kullanılabilir
  - =~ 10.000 satir kod
- Sanallaştırma
  - FreeBSD jail,
  - QEMU/KVM
- Sanal Bağlar :
  - Netgraph
  - Epair
- İzleme
  - Net-SNMP (MRTG)
  - Netflow (nfsen,softflowd)
  - Servis izleme (Nagios)



Kovan'da dört tip sanal cihaz bulunmaktadır. Her ağ cihazı bir sınıfta yer almak zorundadır.

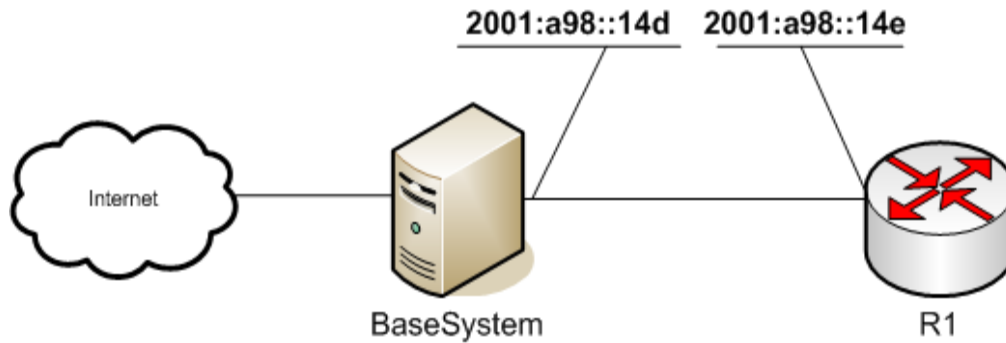
- Yönlendirici (router)
    - Kovan içinde yönlendirme işlemini gerçekleştirir.
  - İstemci (node)
    - Üzerinde servislerin koştığı cihaz tipidir
  - Monitör
    - Kovan'da gerçekleşen tüm aktivitelerin (günlük, bant genişliği kullanımı, paket sayısı, netflow, sanal servislerin ayakta olup olmadığı) bilgisini web arayüzünden verir
  - Karadelik (blackhole)
    - Kovan'a yönlendirilen kullanılmayan IPv6 adreslerine gelen saldırıların kaydını tutar
- Kovan her cihaz sınıfı için gerekli yapılandırma dosyalarını, ilgili programları otomatik olarak kurmakta/oluşturmaktadır.



# Kovan Nasıl Çalışıyor ?

1. Kovan ana yapılandırma dosyası oluşturulur,
  - Bu dosyada Yönlendirici, istemci, bağlantı ve servis tanımları bulunur.
2. Ağda yer alacak yönlendiriciler, sunucular ve istemciler yaratılır.
3. Sanal cihazlar arasındaki sanal bağlantılar yaratılır.
4. Sanal cihazlar arasında tipi yönlendirici olanlar arasında yönlendirme protokolleri çalıştırılır. (RIP, RIPng)
5. Kovan üzerinde koşan gerçek ve sanal servisler çalıştırılır.





physical\_ether: re0  
kovan\_dir: /usr/local/kovan

jail\_roots:  
router: /usr/local/kovan/router

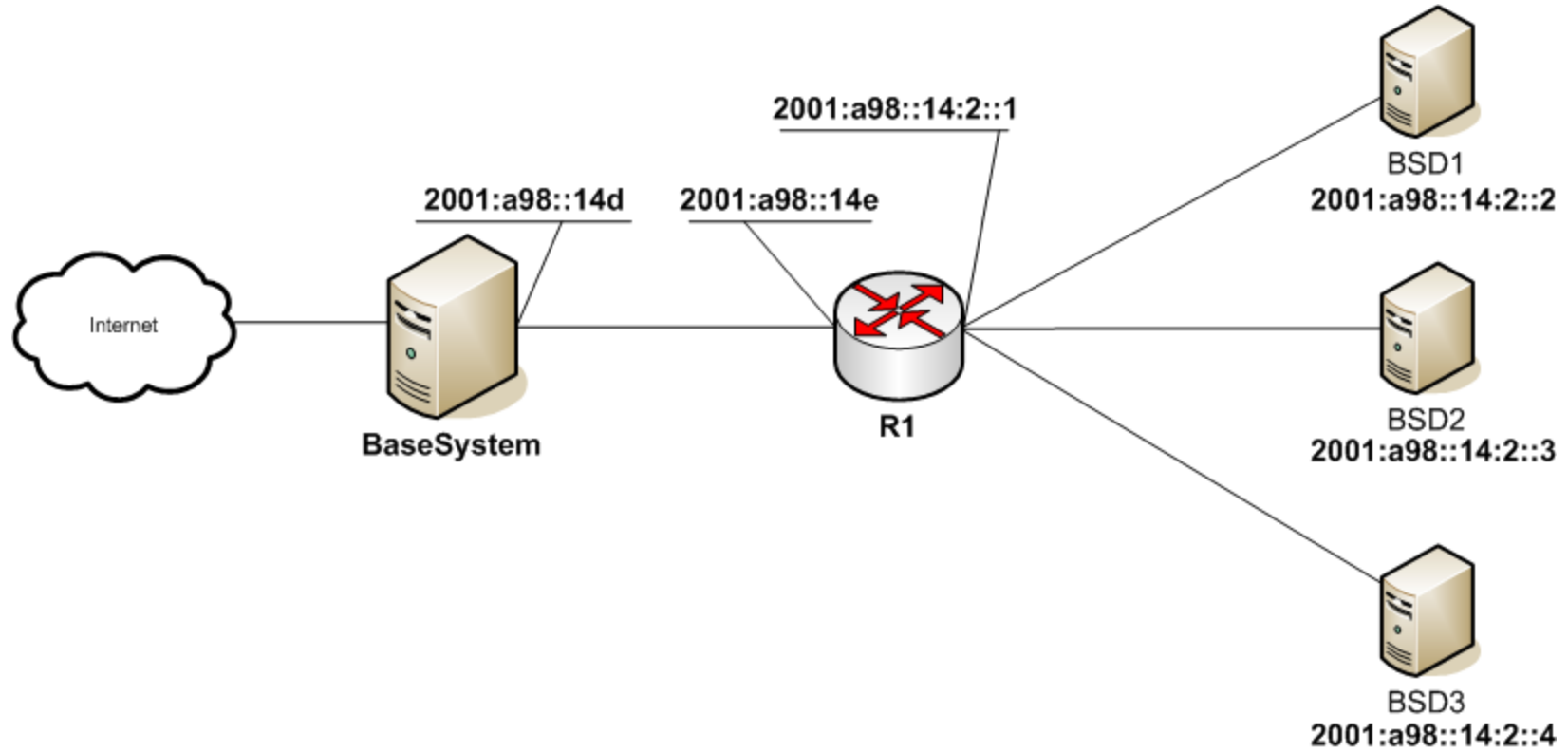
devices:  
- name: localhost  
type: router  
default\_route:  
- "-inet6 -net 2001:a98:14::/48 2001:a98:14::E"

- name: R1  
type: router  
distribute: 1  
default\_route:  
- "-inet6 default 2001:a98:14::D"

connections:

- type: bridge  
peers:  
- name: localhost  
- name: R1  
b\_ip\_address:  
- "-inet6 2001:a98:14::D prefixlen 126"  
n\_ip\_address:  
- "-inet6 2001:a98:14::E prefixlen 126"

# Kovan Senaryo 2



# Kovan Senaryo 2

```
physical_ether: re0  
kovan_dir: /usr/local/kovan  
  
jail_roots:  
router: /usr/local/kovan/router  
node: /usr/local/kovan/node  
monitor: /usr/local/kovan/monitor  
blackhole: /usr/local/kovan/blackhole
```

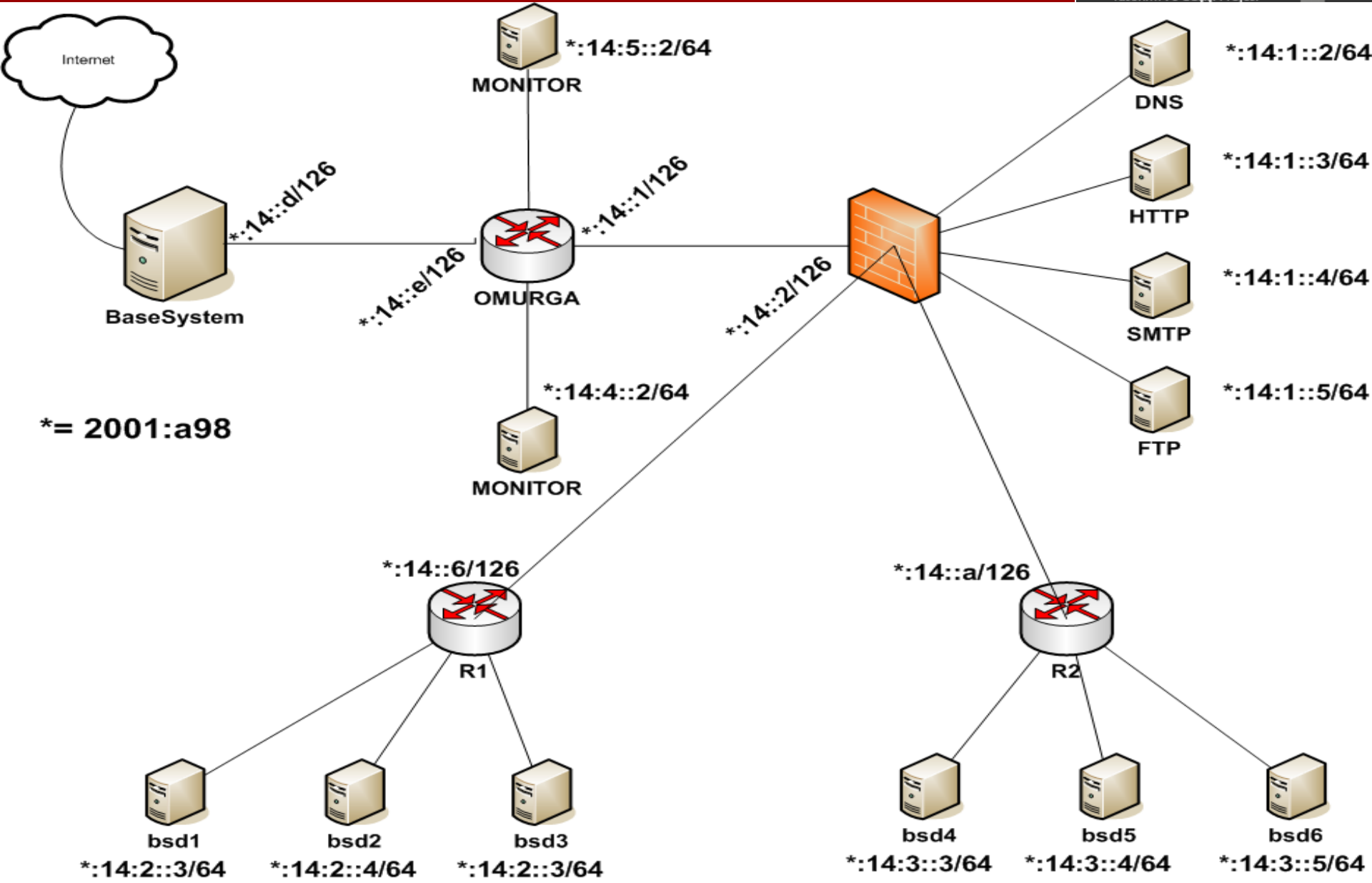
```
devices:  
- name: localhost  
  type: router  
  default_route:  
  - "-inet6 -net 2001:a98:14::/48 2001:a98:14::E"  
  
- name: R1  
  type: router  
  distribute: 1  
  default_route:  
  - "-inet6 default 2001:a98:14::D"  
  
- name: BSD1  
  type: node  
  
- name: BSD2  
  type: node  
  
- name: BSD3  
  type: node
```

connections:

```
- type: bridge  
peers:  
- name: localhost  
- name: R1  
b_ip_address:  
- "inet6 2001:a98:14::D prefixlen 126"  
n_ip_address:  
- "inet6 2001:a98:14::E prefixlen 126"  
  
- type: bridge  
peers:  
- name: R1  
ip_addresses:  
- "inet6 2001:a98:14:2::1 prefixlen 64"  
prefix: "2001:a98:14:2::/64"  
  
- name: BSD1  
ip_addresses:  
- "inet6 2001:a98:14:2::3 prefixlen 64"  
- name: BSD2  
ip_addresses:  
- "inet6 2001:a98:14:2::4 prefixlen 64"  
- name: BSD3  
ip_addresses:  
- "inet6 2001:a98:14:2::5 prefixlen 64"
```



# Kovan Senaryo 3



# Kovan Senaryo 3

```
services:
- name: softflowd
  node: all-routers
  command: /usr/local/sbin/softflowd
- name: cron
  node: MONITOR
  command: /etc/rc.d/cron onestart
- name: snmpd
  node: all-routers
  command: /usr/local/sbin/snmpd -c /etc/snmpd.conf udp6:161
- name: snmpd
  node: BLACKHOLE
  command: /usr/local/sbin/snmpd -c /etc/snmpd.conf udp6:161
- name: syslogd
  node: HTTP
  command: syslogd -P syslog.pid
- name: logger
  node: HTTP
  command: tail -f /var/log/messages | grep kovan | logger -h
2001:a98:14:5::2 -P 510 &
- name: kovan_dns_6
  node: DNS
  command: /usr/local/kovan/bin/kovan\_dns -h {IP6} -p 53 -c
/usr/local/kovan/etc/dns/named.conf -d /usr/local/kovan/etc/dns6.pid
- name: kovan_mail_6
  node: SMTP
  command: /usr/local/kovan/bin/kovan\_smtp -h {IP6} -p 25 -c
/usr/local/kovan/etc/smtp/ipv6go\_mail.conf -d
/usr/local/kovan/etc/smtp6.pid
- name: kovan_http_6
  node: HTTP
  command: /usr/local/kovan/bin/kovan\_http -h {IP6} -p 80 -w
/usr/local/kovan/etc/www/ -d /usr/local/kovan/etc/http6.pid
- name: log_sql
  node: MONITOR
  command: /usr/local/etc/rc.d/mysql-server onestart
- name: syslog
  node: MONITOR
  command: /usr/local/sbin/syslog-ng
- name: flow_logger
  node: BLACKHOLE
  command: /usr/local/kovan/bin/kovan\_dump -i eth0 -f 'ip6 and
host not 2001:a98::173' | logger -h 2001:a98:14:5::2 -P 510 & .
:
```



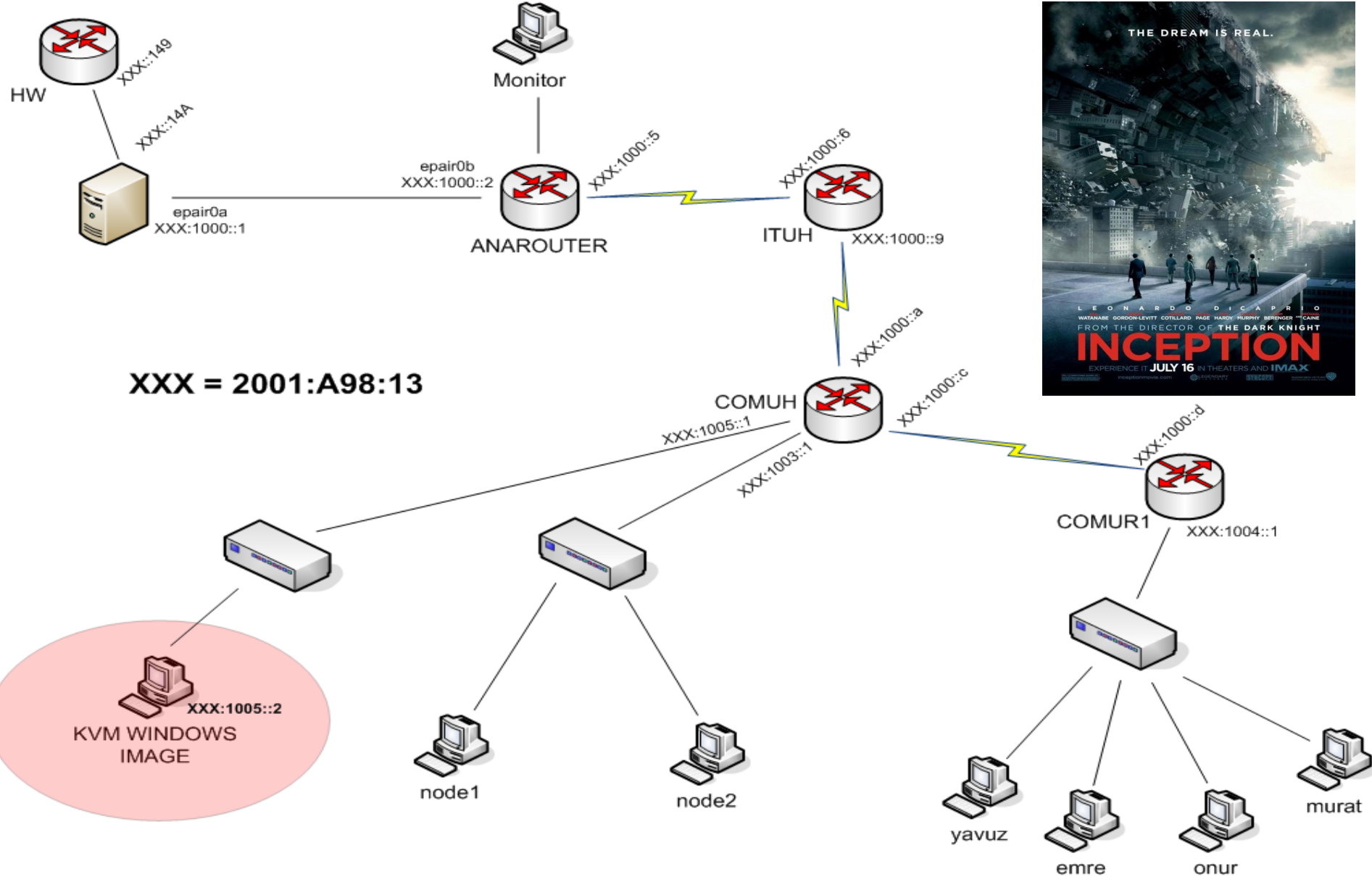
- Durum Kaydetme / Yükleme (Stateful)
  - Kovan yeni bir yapılandırma dosyası ile çalıştırıldığında eski yapılandırma ile ilgili tüm bilgiyi siler
  - Eski bilgiler kovanState komutu ile saklanabilir
  - Durum bilgisi taşıyan tüm dosyalar saklanır, istenildiği zaman aynı veya başka bir sunucuda tekrar yüklenebilir
- İzleme
  - Kovan'ı oluşturan tüm bileşenlere ait gerçek zamanlı bilgiler monitör cihazı web arayüzünden takip edilmektedir.
  - En çok saldırı alan portlar, saldırı alan IP adresleri, en çok saldırı alan portlar, en çok saldırı alan servislere ait grafikler otomatik olarak çizilmektedir
  - Bant genişliği, pps, netflow bilgisi web monitor cihazı web arayüzünden takip edilebilir.



- Sanallaştırma
  - İşletim Sistemi Sanallaştırma
  - Ağ Sanallaştırma
    - Gecikme, bant genişliği, BER değerleri verilebilir.
  - Servis Sanallaştırma
    - Kovan servisleri (HTTP,FTP,DNS,SMTP)
- Dinamik Yönlendirme
  - RIP, RIPng
- Karadelik
  - IPv6 ağları ile birlikte rastgele adres taraması yöntemi ile hedef aranmayacağı öngörülmektedir.
  - IPv6 adres uzayı daraltılarak arama yapılabilir (baba,dede,cafe vb)
  - Rastgele taramaların saptanması için karadelik uygulaması eklenmiştir.
- Günlük
  - Tüm servislere ait günlükler ortak bir formatta veri tabanına kaydedilmektedir.

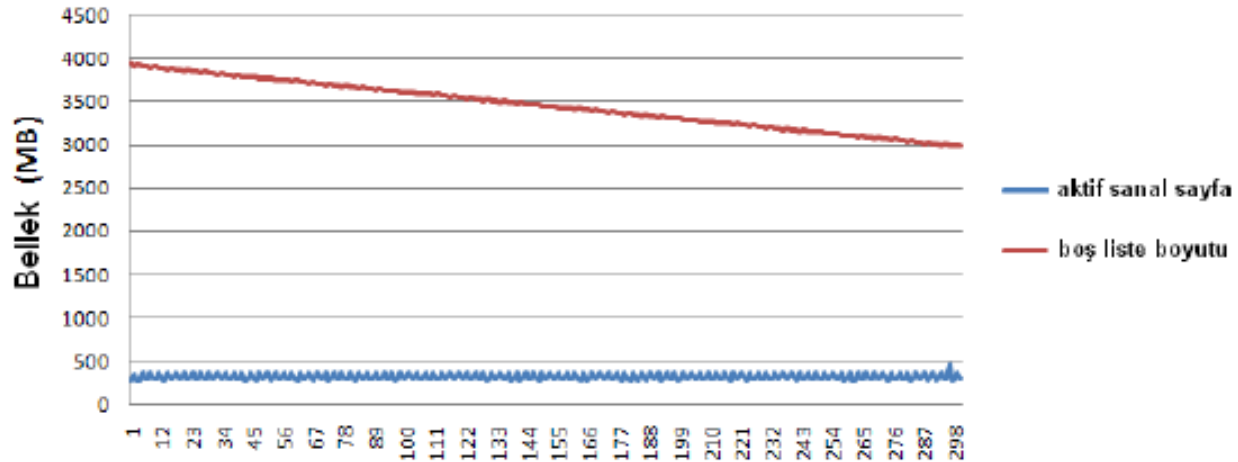


# Rüya içinde rüya/ sanal içinde sanal/ sanal içinde gerçek .....



## •Süreklilik

- Kovan defalarca çalıştırılıp/durdurularak bellek tüketimine ve kararlı çalışabilirliğine bakıldı.



## • Ölçeklenebilirlik

- Sırası ile 16,32,64,128,256 ve 512 cihazlık test senaryoları uygulandı

Cihaz Sayısı	Çalıştırma Süresi	Durdurma Süresi
16	3.26	0.34
32	4.57	0.66
64	6.54	1.34
128	10.55	3.22
256	24.17	7.79
512	52.68	22.2

Tablo I

CIHAZ SAYISI VE KOVAN ÇALIŞTIRMA-DURDURMA SÜRELERİ



## •Stres

- Apache benchmark aracı ab ile 4 istemciden 1.000.000 istek yapıldı

---

```
Concurrency Level:      4
Time taken for tests:   845.515 seconds
Complete requests:     1000000
Failed requests:       42
  (Connect:0, Receive:42, Length:0, Exceptions:0)
Requests per second:   1182.71 [#/sec] (mean)
Time per request:      3.382 [ms] (mean)
Time per request:      0.846 [ms]
                        (mean, across all concurrent requests)
```

### Connection Times (ms)

	min	mean[+/-sd]	median	max
Connect:	0	1 14.4	1	3000
Processing:	0	3 1.1	2	50
Waiting:	0	2 1.0	2	48
Total:	1	3 14.4	3	3004

---



- Kovan'ın ULAKNET ağına konuşlandırıldığı 1 aylık deneme sonucunda:
  - Servislere yapılan herhangi bir saldırı gözlenmedi
  - Rastgele hedef IPv6 adreslerine tarama yapan trafik yakalandı.
  - Kovan karadelik uygulamasınca sıralı ve rastgele IPv6 adresi tarayan üçyüzden fazla IPv6 adresi yakalandı.
  - Hedef portlarda bilinen servisler çalışmıyor
- Bundan sonra;
  - Karadeliğe düşen trafiğin belirli bir düzen izlediği görülmüştür.
  - Kovan bu düzeni tespit ederek taranacak sıradaki IPv6 adresinde bir servis başlatacak şekilde otomatize edilebilir.
  - Servis çalışmayan bir IPv6 adresine saldırı geldiğinde burada servis başlatılabilir.
  - Kovan aldığı saldırı tipine göre otomatik olarak senaryo değiştirecek şekilde yapılandırılabilir (DOS, port tarama vb)



# Son olarak Yavuz'a Hayırlı Tezkereler Diliyoruz



# Sorular ?

Onur Bektas

[onur@ulakbim.gov.tr](mailto:onur@ulakbim.gov.tr)

[bilgi@ipv6.net.tr](mailto:bilgi@ipv6.net.tr)

3122989367

