

Özgür Yazılım Çözümleri Ağ Yönlendirici Cihazı

ODTÜ

hdemir @ metu.edu.tr

TOKEN RING

■ Yıl 1998

- Token Ring sisteminin son zamanları
- Yer yer ethernet kullanılmakta (10 Mbps)
- IBM tarafından kurulan sistem 16 Mbps çalışıyor.
 - Bir iki istisna hariç tüm bölümlerde tek disketlik bir PC router kullanılıyor (Serbest yazılım ☺)
- Ağ sistemleri hala çok özel.
- Bir adet özel sniffer ile dinleme yapılabiliyor ve maliyeti inanılmayacak kadar pahalı.

NASIL BAŞLADI

- Yıl 1999 Cisco 7507
 - Devamlı bir şekilde ağ sorunları çıkmakta.
 - Cisco Türkiye soruna çözüm bulamadı.
 - Cisco Amerika'dan destek oldu.
 - Bize özel yazılım geliştirildi.
 - Ağı kullananlar sistemin çalışmamasına artık alışmışlardı.
 - Sorun ATM'e geçişten dolayı çok yoğun trafik ve accounting hizmeti.

ASKER'deyim.

- Kimse aramadı. Ağ ben yokken iyi mi çalışıyor ☺
- Cisco cihazının yönetim modülü yükseltilmiş.
- ATM ağının maliyeti arttığı için Gigabit Ağ teknolojisine geçiş için hazırlıklar yapılmış.
- Gökhan arkadaşımız FreeBSD manyağı olmuş ☺

YAŞASIN BSD

- Linux'u ilk kurduğum makine 286 idi.
- Yanılmıyorsa bir kernel derlemek çok zaman alıyordu.
 - Sırf kernel parametreleri belirlemek bile bir sorun idi.
 - Kompile olması şimdiler için çok uzun bir zaman alıyordu.
- BSD ile tanışma işi Gökhan ile oldu.

YAŞASIN BSD

- Çok kullanışlı bir işletim sistemi.
- Güvenli.
- Desteklenen.
- Çokça kullanılan.
- Güvenlik duvarı için uygun (özellikle ipfw).
- ATM destekli.
- Kurulum ve yapılandırılması kolay.

DENEMELER

- Askerden geldim.
 - Değişen bir şey yok. Hala Cisco düzgün çalışmıyor.
- İkna çalışmaları.
 - Bu iş olur vs. vs.
 - Sistemin çalışmaması.
 - Yönetimin zaten çözüm istemesi.
 - Diğer maliyetlerin çok olması.
- Devreye alındı.

SORUNLAR

- İşletme sorunları
 - Zebra sorunları
 - Bgpd sorunları
 - ipfw sorunları
 - ipfw2
 - Pf ve ALTQ
- Yönetim sorunları.
- Hardware sorunları.
 - İyi cihazlar IBM tabanlı sunucular
 - Ağ kartı seçimi.
 - İşletim sistemi sürücü sorunları.

GIGABIT'e GEÇİŞ

- Daha sonra ALCATEL alındı.
- OSPF ağı kuruldu.
- Ulakbim ile aramıza F/O kablo çektik.
- Tr-Net ile peering (ATM üzerinden)
- Tr-NET ve arkasındakileri ULAKBİM'e bağlama işi.
- Yukarıda bahsettiğim sorunlardan dolayı Cisco tekrar devreye alındı.
- Verilen pekçok güvenlik hizmeti verilemez oldu.
- Kısıtlı hizmetler. Sadece genel ağ hizmeti verilebildi.

ÇÖZÜM

- Niye linux olmasın.
 - Bir köprü kuruldu.
 - Iptables yapılandırıldı.
 - İç ağ ile Cisco arasına konuşlandırıldı.
- Tüm hizmetler devreye alındı.
 - Asıl amaç IDS idi.
 - snort ve snortsam
 - Güvenlik duvarı – Iptables statefull

KÖPRÜ

- 400 günden fazla uptime
- P2P çalışmalarında ana nokta.
- Güvenlik çalışmalarında ana nokta
- Maliyeti düşük bir ağ güvenlik çözümü.
- Görünmeyen bir yapı.

ULAKBİM BAĞLANTISI

- F/O kablo ile GIGABIT bağlantı
 - Transiever mantıklı olmadı.
 - 100 Mbps tecrübesi
 - Elimizde yedek 3750
 - Pahalı bir çevirici
 - Yararlı
 - Sorunsuz
 - Trafik önceliklendirme kolaylığı
 - Trafik şekillendirme kolaylığı
 - Cisco 7507 Gigabit bağlantı ????

TEKRAR BSD

- FreeBSD 6.x serisi.
- Başlangıçta 3750 kullanıldı.
- Cihaz üzerinde bge kart.
 - BSD bge sürücü sorunları çok yoğun.
 - İşletim sorunları
 - FreeBSD sorunları arttı.
- Yaklaşık 1 yılın sonunda bıraktık.
 - Bu esnada 750 Mpps değerini gördük ☺
 - Tabii ağın çalıştığı söylenemez

ŞİMDİ DURUM

- Yapı itibari ile çok rahatız.
- Pek çok alternatif var.
- Yeni cihazlar aldık. Bunların bir kısmı benzer işler için kullanılıyor.
- Cihazlar ucuz cihazlar değil.
 - Benim masaüstümden pahalı.
 - Bir cisco'dan ucuz.
- IDS olarak yapılandırılan sunucularımız mevcut.
- Cache makinesi

PC SUNUCU

- Ucuz
- İsteddiğiniz kadar RAM – ucuz 😊
- Bilen için işletim kolaylığı.
- IDS olarak yapılandırılabilme.
- Statefull güvenlik duvarı olabilir.
- QoS (ALTQ veya TC)
 - Trafik şekillendirme.
 - Önceliklendirme.
- Üzerinde betik çalıştırabilme.

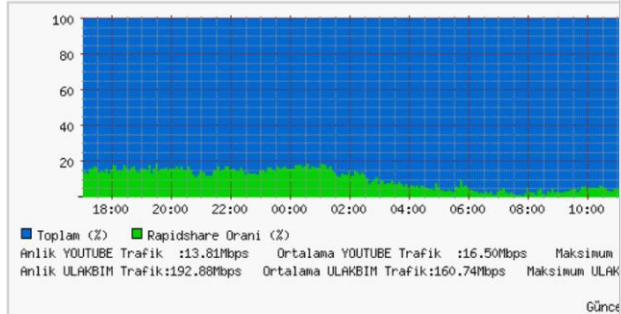
TRAFİK İZLEME

- Üzerinde her türlü trafik izleme olanağı var.
- RRDTOOL
 - Çok başarılı
 - Kullanımı kolay
 - Grafik üretmek için çeşitli betikler yazıldı
- IPTABLES verileri ile istenilen trafik izlenebilmektedir
- LOG yönetimi
 - Swatch
 - Kendi yazdığımız betikler
- fprobe-ng
 - flow-tools ile işlenebilecek
 - Netflow verileri üretiyor

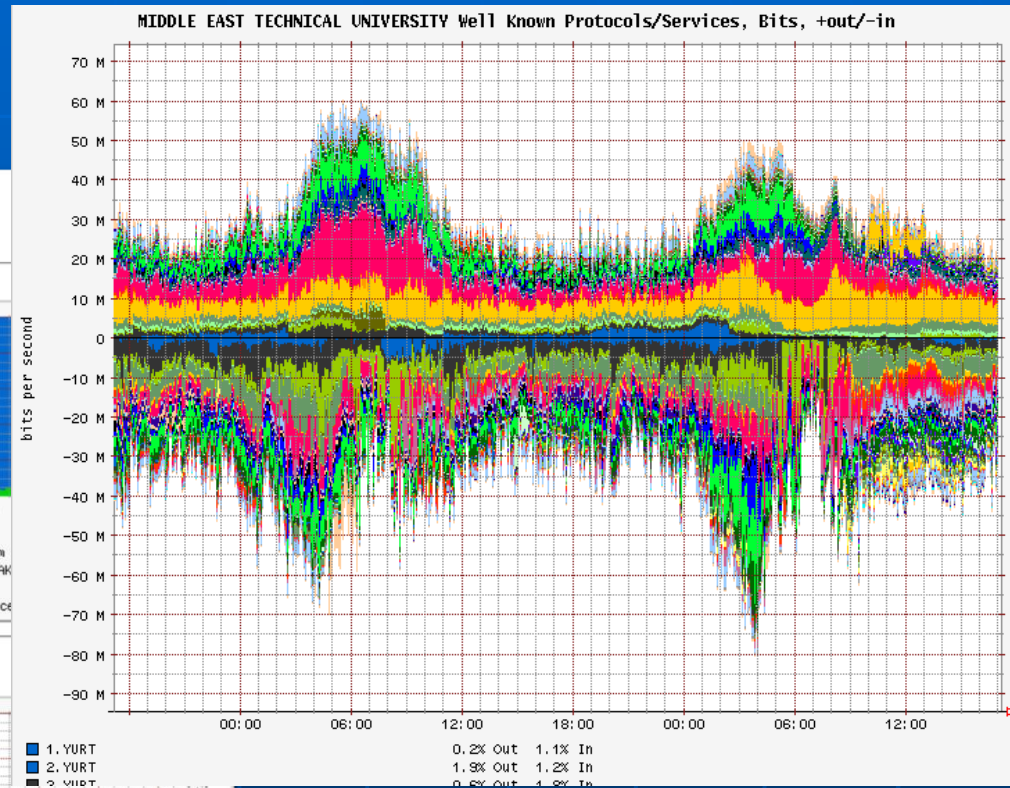
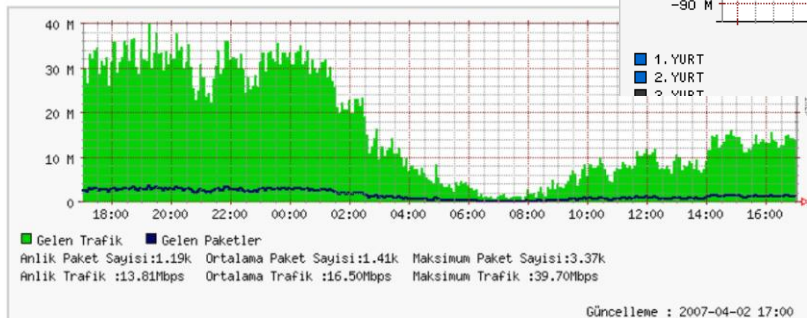
TRAFİK İZLEME

YOUTUBE Kullanım İstatistikleri

YOUTUBE Kullanımının Kampüs Çıkışına Oranı (%)



Günlük kullanım istatistikleri:



IPTABLES

- Bağlantı izleme – CONNTRACK
 - Devamlı gelişme
- IPTABLES çok ama çok başarılı
- IPSET yapılandırıldı.
 - 20 000 IP adresi eklenebiliyor.
 - Cisco'da nasıl olduğunu siz düşünün.
 - Bu sadece bir tablo !!!
- Linux eksikliği SYN proxy ???
 - TARPIT
- STRING eklentisi
- CONNLIMIT
- ROUTE

IPv6

- Pekçok ticari yönlendiricide yeni destekleniyor.
- BSD, Linux vs. üzerinde çoktan beri var.
- IPv6 güvenlik duvarı yapılabiliyor. ☺
- Gelecek teknolojilere açık.
- Üzerindeki servislerin IPv6 desteği var.

