

Linux Üzerinde İleri Düzey Güvenlik Duvarı Uygulamaları

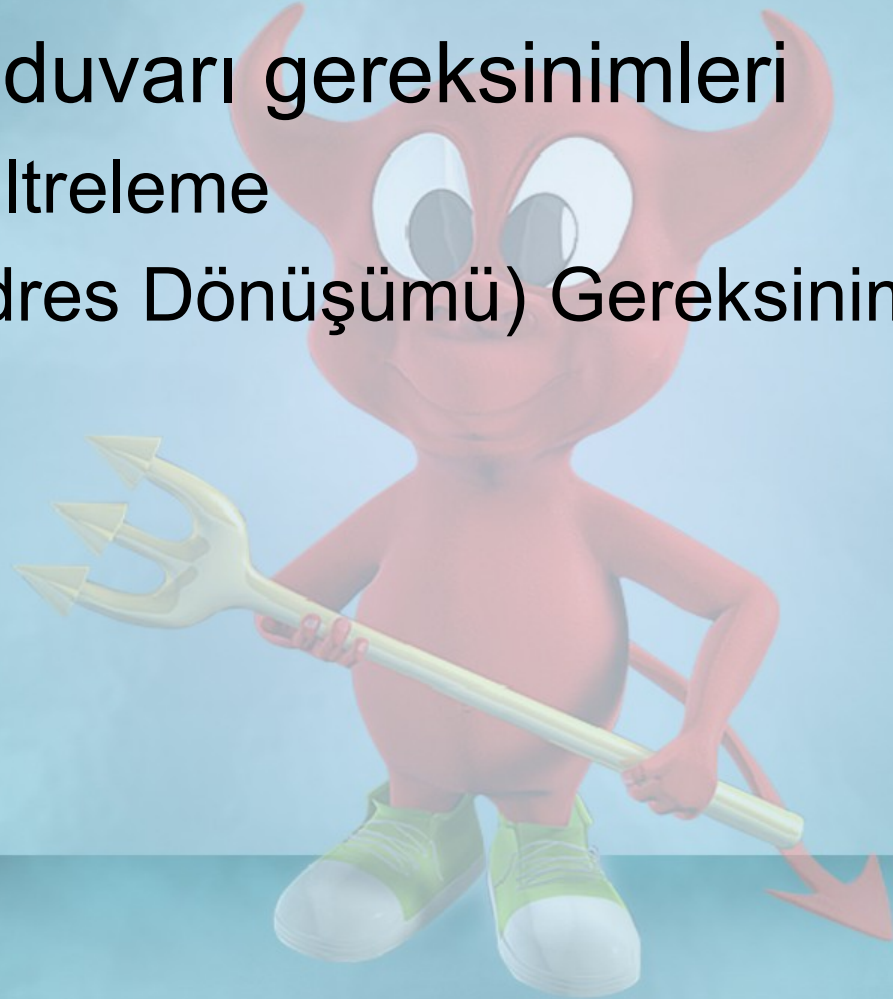
Afşin Taşkiran
EnderUnix YGT ~ Türkiye
Çekirdek Takımı Üyesi
afsin ~ enderunix.org
www.enderunix.org/afsin

Sunum Planı

- Standart Güvenlik Duvarı Yapısı
- Iptables ile paket filtreleme ve NAT işlemleri
- Patch-o-matic
- L2 seviyesinde güvenlik duvarları
- ebttables ile L2 paket filtreleme
- Uygulama seviyesinde paket filtreleme
- L7-filter ile güvenlik duvarı işlemleri
- Linux ile trafik kontrolü ve QOS
- Cluster yapıda Linux güvenlik duvarı

Standart Güvenlik Duvarı Yapısı

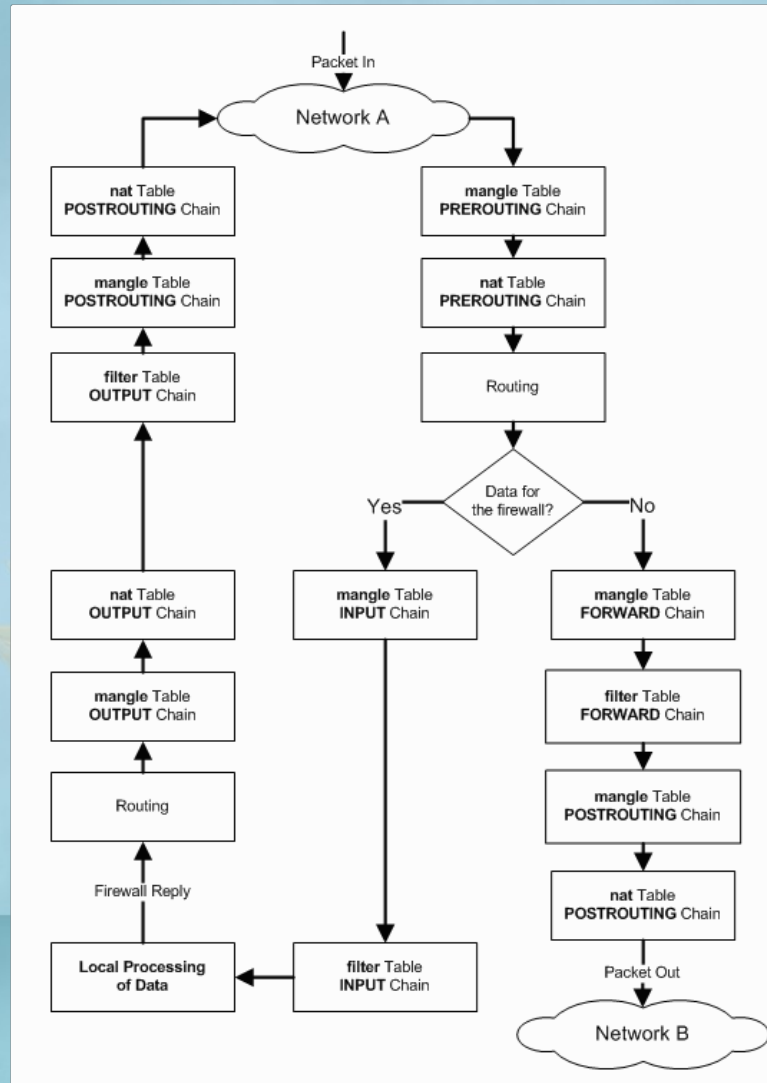
- Güvenlik duvarı gereksinimleri
 - Paket Filtreleme
 - NAT (Adres Dönüşümü) Gereksinimi



Iptables ile paket filtreleme

- İlgili paketlerin tanınması
 - IP/TCP Katmanında tanımlama (Kaynak/Hedef v IP/Port)
 - -s 192.168.0.67
 - -d 10.1.1.34 –p tcp
- Gerekli işlemlerin yapılması
 - Kabul (ACCEPT), Reddetme (DROP), Geri Gönderme (REJECT)
 - -j ACCEPT
 - -j DROP
 - -j REJECT

Iptables ile paket filtreleme



Iptables ile NAT İşlemleri

- IP Paketindeki Kaynak/Hedef – IP/Port bilgilerinin değiştirilmesi
 - iptables –t nat –A POSTROUTING –o eth1 –j SNAT –to-source 192.168.1.67
 - İptables –t nat –A PREROUTING –i eth1 –p tcp –d 192.168.1.67 –dport 80 –j DNAT –to-destination 10.0.0.34:8080

Paket Yönlendirme ve NAT

- Paket trafiğinin ağ arayüzleri arasında aktarılması
- NAT işlemine tabi tutulan paketin ilgili ağ katmanına gönderilmesi
- NAT işlemi ile birlikte paket yönlendirme gereksinimi

patch-o-matic

- Iptables'ın geliştirilmekte olan modüllerinin ilk aktarıldığı ortam
- Test deposu olarak da kullanılıyor.
- Yeni teknolojilerin test ortamı
- 30'a yakın yeni eşleşme türü
- 10 tane yeni eylem

patch-o-matic : Eşleşmeler (matches)

- TTL Yaması
 - iptables -A INPUT -m ttl --ttl-lt 5 -j LOG
- Zaman Yaması
 - iptables -A INPUT -m time --timestart 8:00 --timestop 18:00 --days Mon,Tue,Wed,Thu,Fri -j ACCEPT
- String eşleşmesi
 - iptables -A INPUT -m string --string 'cmd.exe' -j QUEUE
- Kota Yaması
 - iptables -A INPUT -p tcp --dport 80 -m quota --quota 52428800 -j ACCEPT
 - iptables -A INPUT -p tcp --dport 80 -j DROP

patch-o-matic : Eşleşmeler (matches)

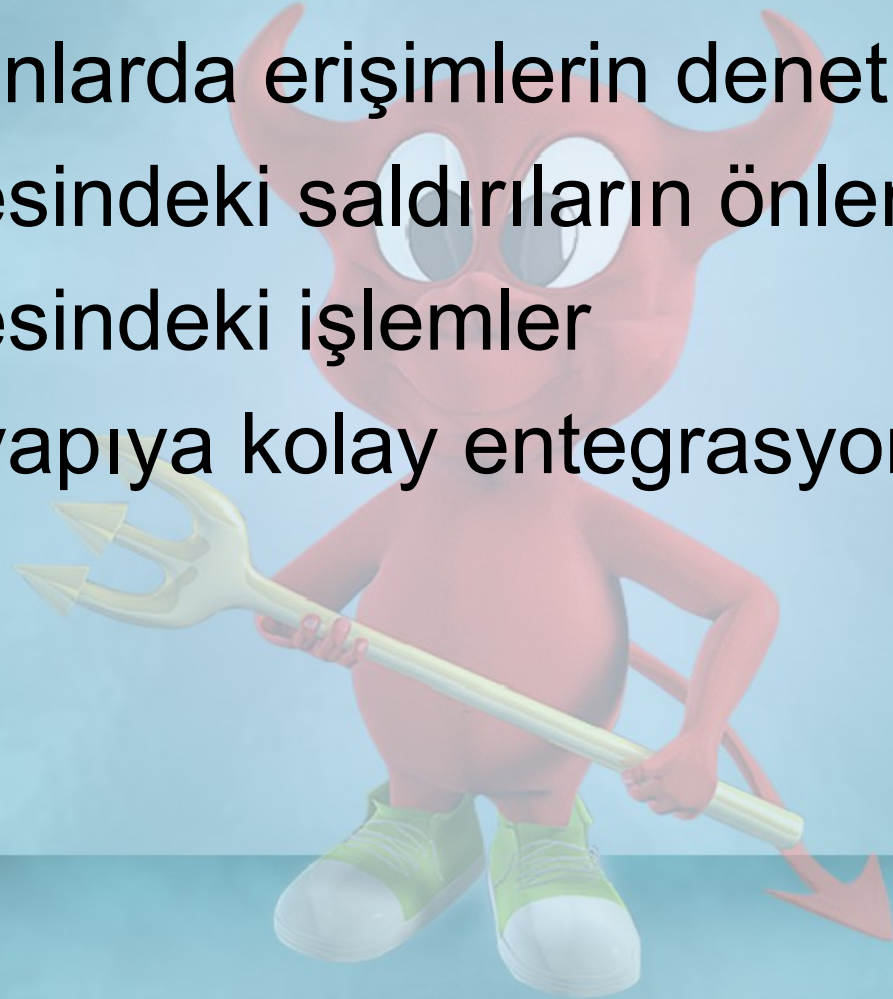
- Port taramalarının tanımlanması (psd yaması)
 - iptables -A INPUT -m psd -j DROP
- Paket türü yaması (host, broadcast, multicast)
 - iptables -A INPUT -m pkttype --pkt-type broadcast -j DROP
- Mport Yaması
 - iptables -A INPUT -p tcp -m mport --ports 20:23,80 -j DROP
- Paket genişliği yaması
 - iptables -A INPUT -p icmp --icmp-type echo-request -m length --length 86:0xffff -j DROP

patch-o-matic : Eylemler (Targets)

- ftos Yaması
 - iptables -t mangle -A OUTPUT -j FTOS --set-ftos 15
- Netlink Yaması
 - Tüm paketleri DROP edip kullanıcı tarafında netlink soketleriyle dönüş
 - Paketin işaretlenmesi, paket büyüklüğünün değiştirilmesi
 - iptables -A INPUT -p icmp --icmp-type echo-request -j NETLINK --nldrop
- tcp-MSS yaması
 - TCP bağlantıların maksimum büyüklüğünün kontrolü
 - iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
 - --set-mss value
 - --clamp-mss-to-pmtu
- TTL Yaması
 - iptables -t mangle -A OUTPUT -j TTL --ttl-set 126

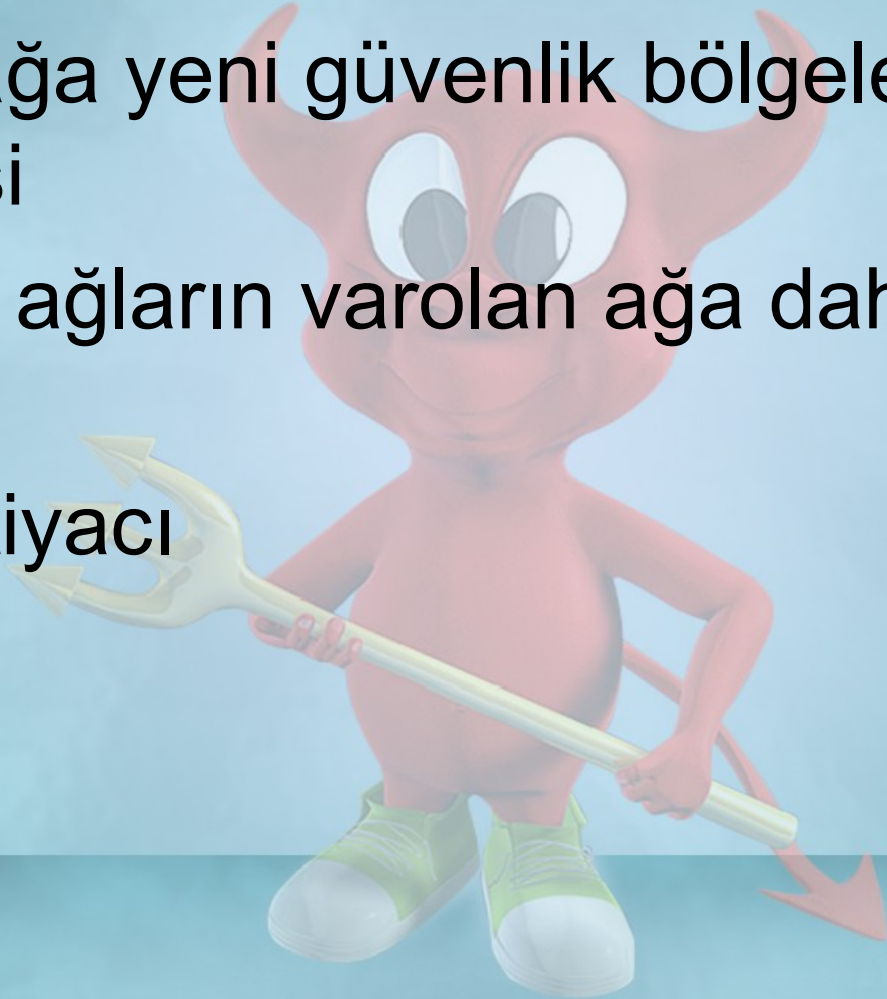
L2 Seviyesinde Güvenlik Duvarları

- Alt katmanlarda erişimlerin denetlenmesi
- L2 seviyesindeki saldırıların önlenmesi
- L2 seviyesindeki işlemler
- Varolan yapıya kolay entegrasyon



L2 Seviyesinde Güvenlik Duvarları: *Pratik Uygulamalar*

- Varolan aęa yeni güvenlik bölgelerinin eklenmesi
- Kablosuz aęların varolan aęa dahil edilmesi
- Gizlilik ihtiyacı



L2 Seviyesinde Güvenlik Duvarları:

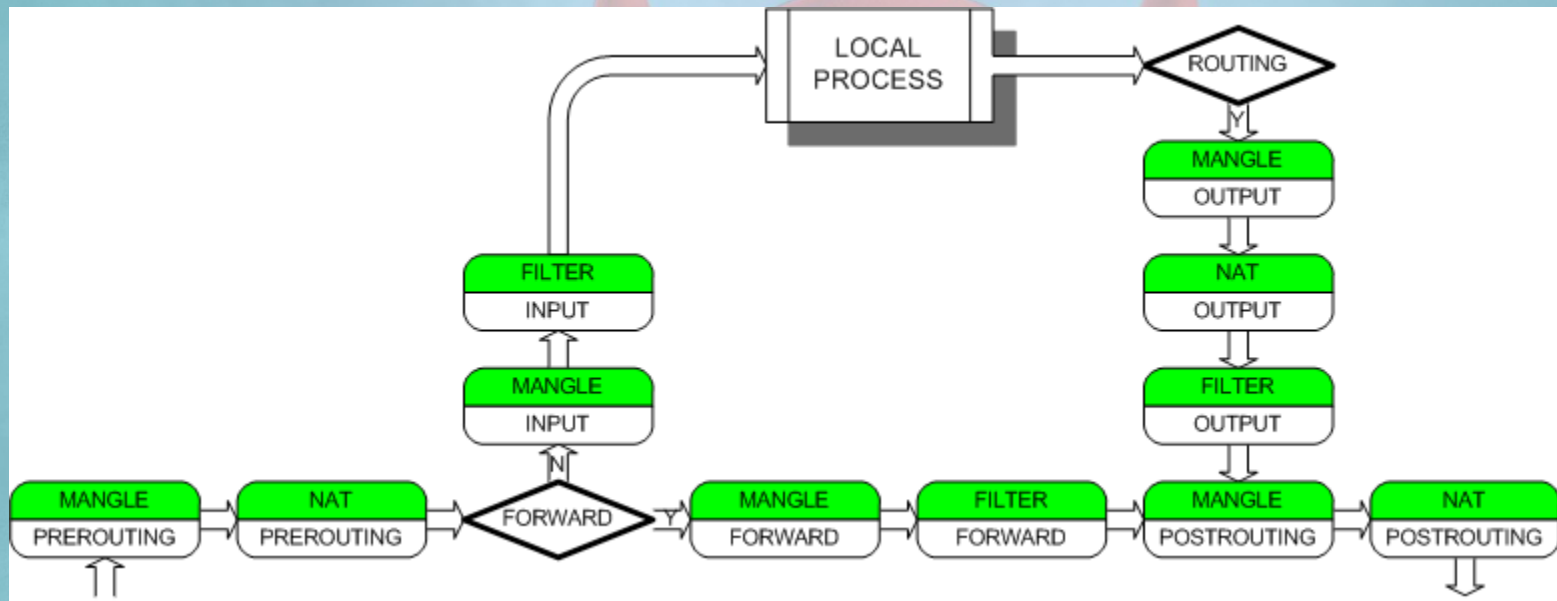
br-nf

- Linux sistemlerin köprü modunda çalışması
- Güvenlik duvarı arabirimi ile entegrasyon
- IP katmanında çalışmaz, IP yok
- Yönlendirme yapılmaz

L2 Seviyesinde Güvenlik Duvarları: *ebtables*

- L2 paket filtreleme (ethernet, 802.1q, 802.3)
- ARP işlemleri
- L3 filtreleme
- Netfilter ile tam entegrasyon
- L2 NAT işlemleri
- Kayıt tutabilme, paket işaretleme
- iptables'a benzer söz dizimi ile kullanabilme

L2 Seviyesinde Güvenlik Duvarları: *iptables*



L2 Seviyesinde Güvenlik Duvarları: *ebtables*

- Özel bir mac adresi için sadece IPV4 sınıfı IP kullanımına izin verilmiş, diğer türler yasaklanmıştır.
 - `ebtables -A FORWARD -s 00:11:22:33:44:55 -p IPV4 -j ACCEPT`
 - `ebtables -A FORWARD -s 00:11:22:33:44:55 -j DROP`
- Hedefi 00:11:22:33:44:55 olan paketlerin hedef adresini 54:44:33:22:11:00 olarak değiştirmek
 - `ebtables -t nat -A PREROUTING -d 00:11:22:33:44:55 -i eth0 -j dnat --to-destination 54:44:33:22:11:00`

Uygulama Seviyesinde Paket Filtreleme : I7-filter

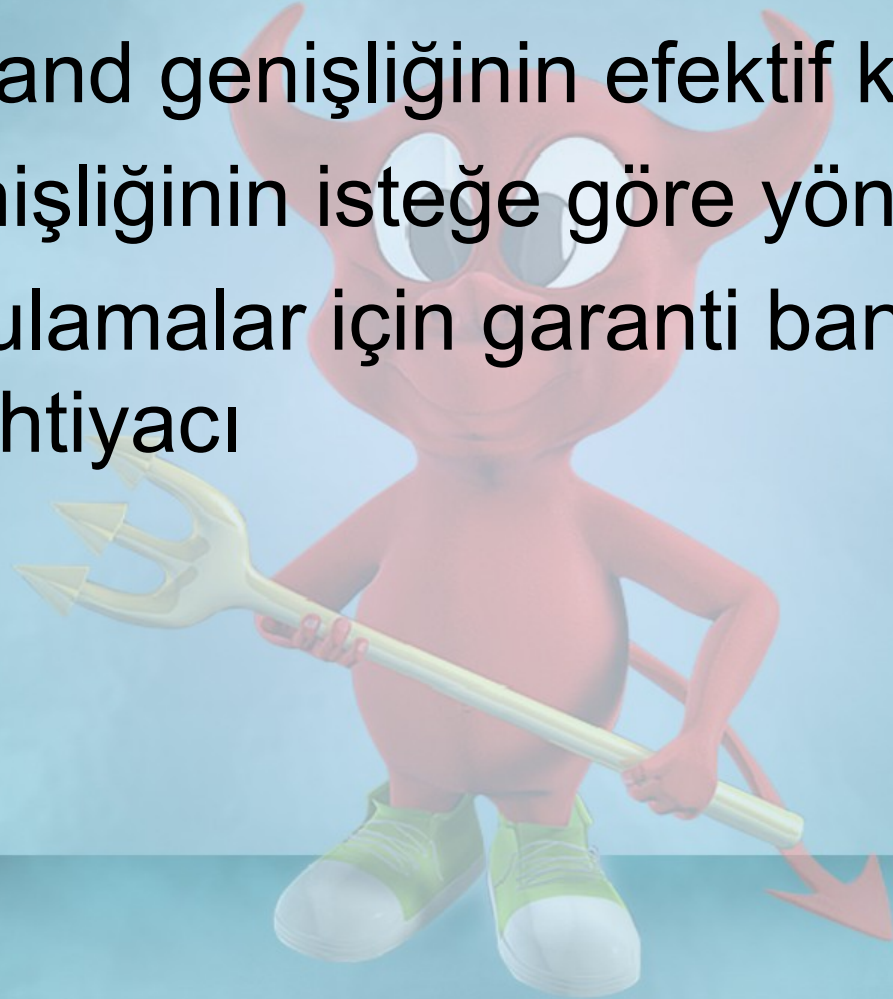
- Netfilter için uygulama seviyesinde paket sınıflandırıcı
- TCP, UDP, ICMP desteđi
- Çoklu paket karşılaştırma özelliđi
- QoS uygulamaları
- Formlardaki betikleri, resimleri, metinleri **ANLAMLANDIRMAZ !**

Uygulama Seviyesinde Paket Filtreleme : I7-filter

- Paket tanımlama
 - P2P trafiğın tanımlanması (<http://ipp2p.org/>)
 - Protokol veritabanının kullanılması (protocolinfo.org)
 - P2P protokolleri
 - Anlık mesajlaşma protokolleri
 - Oyun protokolleri
 - VoIP Protokolleri
 - RFC ler ile protokol tanımları
 - Virusler ve casus yazılımlar
 - Sınıflandırılmamış protokoller
 - Kendi protokollerinizi tanımlayabilirsiniz
 - Düzenli ifadeler ile paket tanımlama

Linux ile Trafik Kontrolü ve QoS

- Mevcut band genişliğinin efektif kullanımı
- Band genişliğinin isteğe göre yönetilmesi
- Bazı uygulamalar için garanti band genişliği ihtiyacı
 - VoIP



Linux ile Trafik Kontrolü ve QoS

- Kernel qos modulleri
 - CBQ Packet Scheduler
 - U32 Classifier
 - SFQ Queue
 - TBF Queue
- tc
- tc-filter
- tc-cbq
- tc-spq
- tc-tbf



Cluster Yapıda Linux Güvenlik Duvarı

- UCARP Projesi
 - Sanal IP lerle yük paylaşımı sağlanması
 - CARP (Common Address Redundancy Protocol)
 - OpenBSD'nin CARP'ı, VRRP'nin alternatifidir.
 - Multicast adreslerle diğer makineyi kontrol
 - Oturum ve RTO paylasimi yapilmaz

Kaynaklar

- http://www.skyfree.org/linux/kernel_network/netlink.html
- <http://www.enderunix.org/afsin/belgelerim/linuxbridgemo de.pdf>
- <http://www.netfilter.org/>
- <http://ebtables.sourceforge.net/>
- <http://lartc.org/>
- <http://protocolinfo.org>
- <http://l7-filter.sourceforge.net/>
- <http://www.ucarp.org>
- www.enderunix.org/docs
- www.enderunix.org/afsin/blog

Teşekkürler

Linux Üzerinde İleri Düzey Güvenlik Duvarı
Uygulamaları

Afşin Taşkıran

EnderUnix Çekirdek Takımı Üyesi
afsin ~ enderunix.org

Resmi Sponsorumuz: **EnderSys** Yazılım Danışmanlık
www.endersys.com.tr

