Özgür Yazılımlarla Sınır Güvenliği

Huzeyfe ÖNAL

huzeyfe@lifeoverip.net

http://www.huzeyfe.net

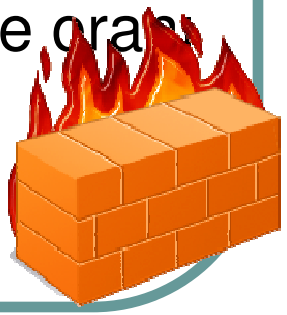
Complexity is the Enemy of Security... (Anonymous)

Sunum Planı

- Sınır Güvenliği Bileşenleri
  - Yönlendiriciler(router)
  - Güvenlik Duvarları(Firewall)
  - Saldırı tespit/Engelleme sistemleri(IDS/IDP)
  - Kablosuz Erişim Noktaları(WAP)
  - Sanal Özel Ağlar(VPN)
- Sınır Güvenliğinde Alternatif Özgür yazılım Uygulamaları

Sınır Koruma Evrimi

- Sınır Güvenliği...
- Routerler üzerine yazılan erişim kontrol listeleri(ACL)
- Güvenlik duvarlarının gelişimi
  - Durum korumasız güvenlik duvarları
  - Durum korumalı(Stateful packet inspection)
- Saldırı Tespit Sistemleri(IDS)
  - Pasif , sensor tabanlı , kompleks, false positive oranı yüksek.. Sonuç?.
- Saldiri tespit ve Engelleme (IDP) Sistemler
  - Aktif, Protokol analizi, anormallik sezinleme,



Durum Korumalı Güvenlik duvarları ile Koruma

- Kaynak:
  - Paket nerden geliyor?
- Hedefe:
  - Nereye gidiyor?
- Servis:
  - Hangi servis/port için incelenecek?
- Oturum:
  - Oturum başlatan kim? Gelen paket hangi oturuma ait?
  - TCP Bayrakları bağlantı aşamasına uygun mu?..

??Sonuç ??

Açık Kod Güvenlik Duvarları

- OpenBSD Packet Filter
- FreeBSD IPF, IPFW, PF
- Linux iptables

- Karşılaştırma Tablosu >>

	IPFW(FreeBSD)	PF(Free/Net/Open BSD)	IPF(FreeBSD)	IPTABLES(Linux)
Stateful Inspection	Var	Var	Var	Var
IPsec VPN Özelliği	Var(OS)	Var(OS)	Var (OS)	Var(OS)
Basit IDS/IPS Özelliği barındırma	Yok	Var	Var	Var
Layer 2 de çalışabilme (Bridge)	Var	Var		Var
Load Balancing Desteği	Var	Var	Yok	Yok
HA çalışabilirlik(Failover)	Yok	Var	Var	Yok
Yönetim - CLI, WEB, GUI -	qtfw	pfw, FwBuilder, pfcli	...m0n0wall	fwbuilder,
Loglama ve Raporlama Yeteneği	Syslog	Binary and Syslog*	Syslog, Text file	Syslog
Trafik şekillendirme, QOS desteği	Var - dummynet & altq	Var - altq	Yok (AltQ ile yapilabil	Var
Politika tabanlı Yönlendirme	Var	Var	Yok	Yok
Kullanıcı bazlı kural uygulama	Var	Var	Var	Yok
Logları merkezi bir sisteme gönderme	Var(Syslog)	Var (dup-to/syslog)	Var (Syslog)	Var (Syslog)
Antispoofing Özelliği	Var	Var	Var	Yok
MAC tabanlı filtreleme özelliği	Var	Var (L2 modda)	Yok	Var
IPv6 desteği	Var	Var	Var	Var
Tablo desteği	Var	Var	Yok	Yok
Kural başı bağlantı limiti	Var	Var	Var	Var
Verify Source Reachable özelliği	Var	Var	Yok	Yok
Netgraph'a yönlendirme desteği	Var	Yok	Yok	Yok
Divert socketlerine yönlendirme desteği	Var	Yok	Yok	Yok
Local Forwarding Özelliği	Var	Yok	Var	Yok
Ruleset desteği	Var	Var	Var	Var
probability (paketlerin düşürülme ihtimalleri)	Var	Var	Yok	Yok
passive os fingerprinting	Yok	Var	Yok	Yok
limit state per rule	Var	Var	Yok	?
tos	Var	Var	Yok	Var

Iletişim Adresi: staff@enderunix.org

OpenBSD PF(Packet filter)

- En gelişmiş açık kod Firewall çözümü
- Aktif gelişim süreci
- Kolay ve anlaşılır yapı
- HA ve Load Balancing
- Ileri düzey trafik kontrolü
- Bandwidth Shaping
- Bridge mode çalışma yeteneği
- Üstün performans
  - Gerçek hayattan örnekler
- Iptables mi Packet Filter mi?

OpenBSD Firewall Technical Specifications v0.3

Networking

- Advanced routing protocols, including BGP,OSPF, RIP
- GRE tunneling
- Source Based Routing
- 802.1Q VLAN support
- Traffic shaping (QoS)
- Unicast Reverse Path Forwarding(URPF)

HA and Load Balancing

- Firewall Failover with pfsync and CARP
- VPN/Firewall session synchronization
- Encrypted HA Traffic
- Redundant Interface with Trunk
- ISP Load Balancing

Firewall

- Dynamic Stateful inspection firewall
- Nat (Network Address Translation)
- PAT (Port Address Translation)
- Policy Based Routing
- Malformed Packet Protections
- DOS Prevention with syn proxy
- User based rules / User Authentication
- Bandwidth management
- Policy Filtering(Packet Tagging)
- Layer 2 Mode (Transparent Mode) Firewalling
- Passive Operating System Fingerprinting

VPN

- IPSec VPN tunneling with DES/3DES/AES encryption
- Ipsec NAT Traversal
- Dead peer detection
- Pre-shared secrets

Logging

- Pcap formatted fast logging
- Multiple Log target
- Logging to a syslog server

Huzeyfe ÖNAL
<huzeyfe@enderunix.org>
18.12.2006

OpenBSD PF -II

- GUI aracılığı ile yönetim
  - Fwbuilder
  - PFW
- Örnek kural söz dizimi

Filtreleme;

Block in log on $ext_if proto tcp ftom any to 172.16.10.1 port 23

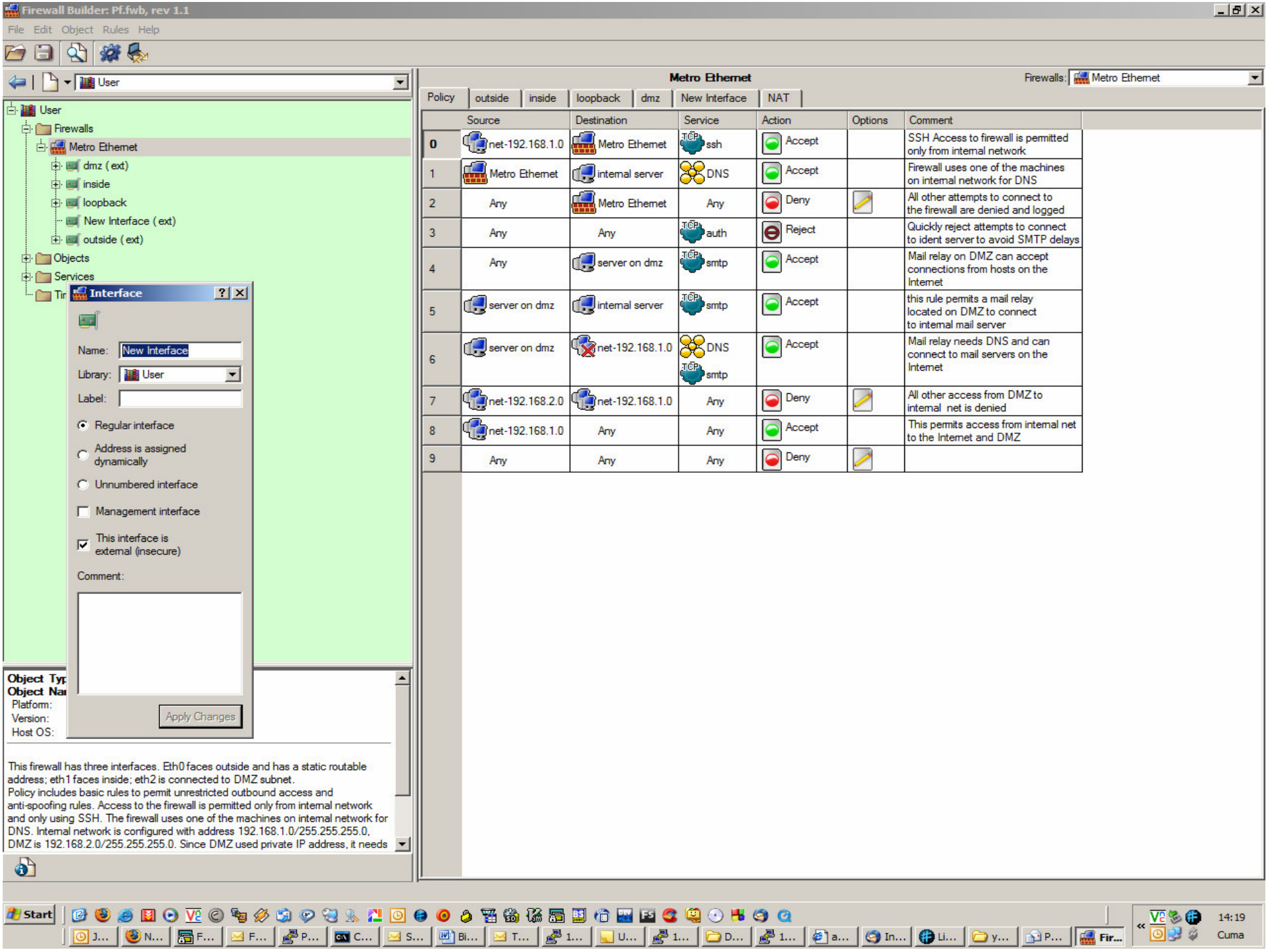
Nat;

Nat on $ext_if from $ic_ag to any -> 11.22.33.44

- Basit, performanslı, anlaşılır log yapısı
- Tcpdump kullanılarak izlenebilir.

Dec 02 17:20:31.046452 pass out on fxp0: 15.1.5.74.52741 : 83.41.39.166.4672: tcp

- Web arabiriminden rapor alınabilir


Firewall Builder: Pf.fwb, rev 1.1
File Edit Object Rules Help
User
Firewalls
Metro Ethernet
dmz (ext)
inside
loopback
New Interface (ext)
outside (ext)
Objects
Services
Interface
Name: New Interface
Library: User
Label:
Regular interface
Address is assigned dynamically
Unnumbered interface
Management interface
This interface is external (insecure)
Comment:
Apply Changes
Platform:
Version:
Host OS:
This firewall has three interfaces. Eth0 faces outside and has a static routable address; eth1 faces inside; eth2 is connected to DMZ subnet.
Policy includes basic rules to permit unrestricted outbound access and anti-spoofing rules. Access to the firewall is permitted only from internal network and only using SSH. The firewall uses one of the machines on internal network for DNS. Internal network is configured with address 192.168.1.0/255.255.255.0, DMZ is 192.168.2.0/255.255.255.0. Since DMZ used private IP address, it needs
Metro Ethernet
Firewalls: Metro Ethernet
Policy outside inside loopback dmz New Interface NAT
Source Destination Service Action Options Comment
0 net-192.168.1.0 Metro Ethernet ssh Accept SSH Access to firewall is permitted only from internal network
1 Metro Ethernet internal server DNS Accept Firewall uses one of the machines on internal network for DNS
2 Any Metro Ethernet Any Deny All other attempts to connect to the firewall are denied and logged
3 Any Any auth Reject Quickly reject attempts to connect to ident server to avoid SMTP delays
4 Any server on dmz smtp Accept Mail relay on DMZ can accept connections from hosts on the Internet
5 server on dmz internal server smtp Accept this rule permits a mail relay located on DMZ to connect to internal mail server
6 server on dmz net-192.168.1.0 DNS smtp Accept Mail relay needs DNS and can connect to mail servers on the Internet
7 net-192.168.2.0 net-192.168.1.0 Any Deny All other access from DMZ to internal net is denied
8 net-192.168.1.0 Any Any Accept This permits access from internal net to the Internet and DMZ
9 Any Any Any Deny
Start
14:19
Cuma

Zararlı Paketlerle Mücadele

- Nmap, hping, firewallk vs gibi araçların kontrolü- Sihirli Sözcük ?
- Scrubbing
  - no-df
  - min-ttl
  - fragment reassemble

**scrub in on fxp0 all fragment reassemble min-ttl 15 **
max-mss 1400 no-df

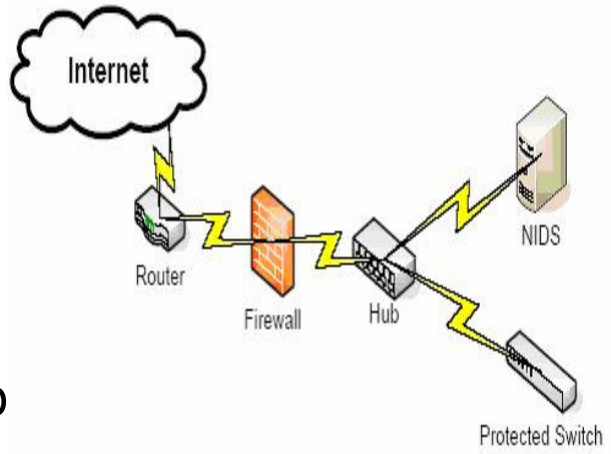
- POSF(**Passive Operating System Fingerprinting**)
  - pass in on $int_if from any os OpenBSD keep state
    block in on $int_if from any os "Linux 2.6"
  - block in on $int_if from any os "Windows Vista"

(N)IDS, (N)IPS, Inline, Active Response Tanımları

- IDS – Intrusion Detection System
  - Pasif Koruma
  - Active Response
  - NIDS, HIDS, WIDs, DIDS
- IPS – Intrusion Protection System
  - Aktif Koruma –Inline Sistem
  - NIPS, HIPS
- False Positive, False Negative
- Sensor, Agent, Korelasyon,

IDS/IPS Yerleşimi

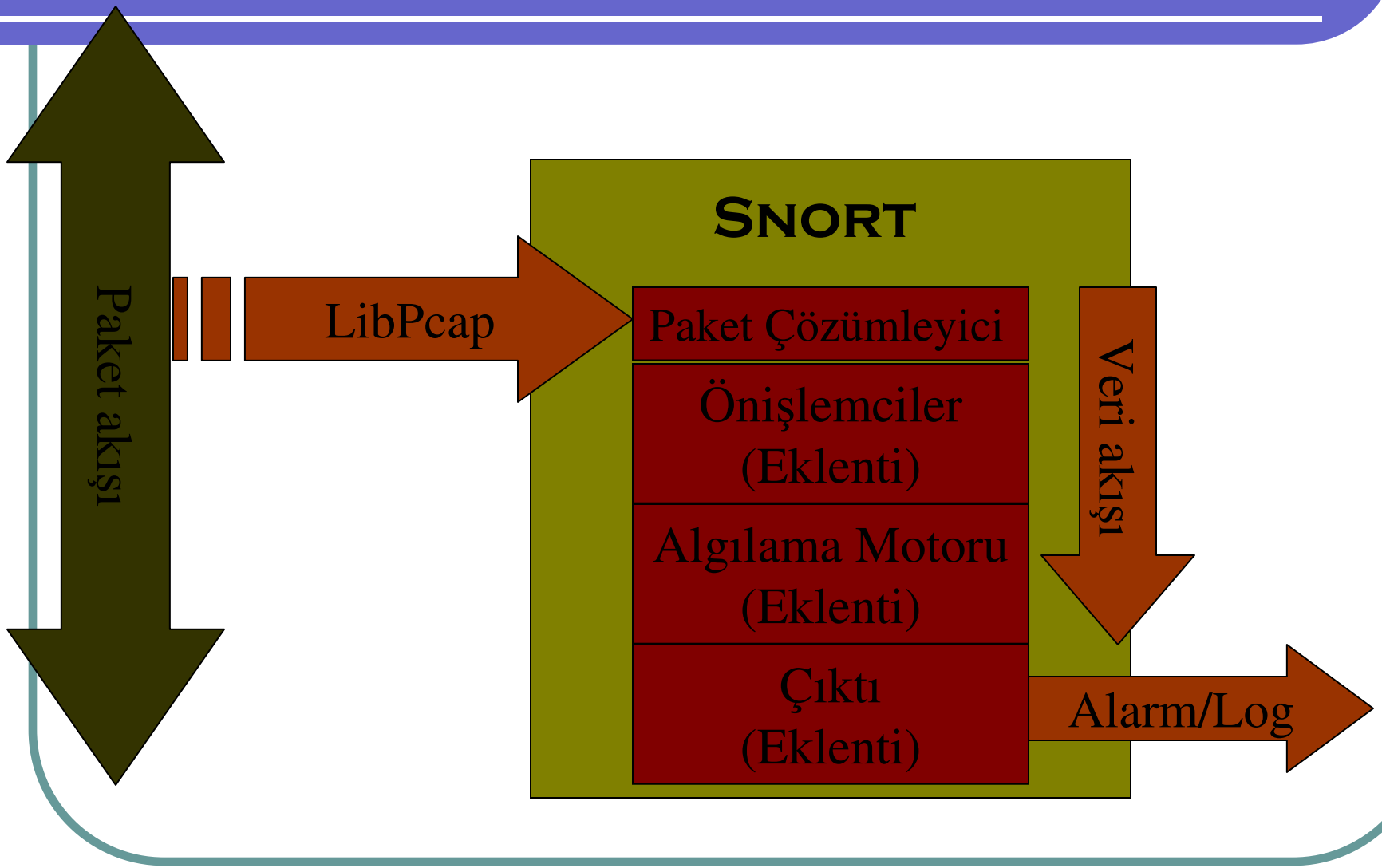
- Ağın durumuna göre yerleşim önemli
- Firewall Önü
  - Yüklü miktarda uyarı, gereksiz trafik
  - Tehditleri daha iyi belirler
- Firewall arkası
  - Sadece FW'an geçen paketler, trafik yo
  - Tehditleri daha az belirleyebilir.
- Switch Span portu, özel network tap cihazları(Internal)
  - Linux/BSD yüklü sağlam sunucu



Snort: Açık Kodlu Atak Engelleme Sistemi

- Açık Kaynak Kodlu, Özgür Lisansa Sahip
- ’98 yılında hobi amaçlı başlangıç
- Günümüzde: akademik, askeri, ticari kullanım alanları
- Sniffer & Logger
- (N)IDS/(N)IPS/(N)IDP
- Forensic Analiz Aracı
- Linux/UNIX/Windows
- Stateful Packet Tracki
- Hedef tabanlı IDS öze

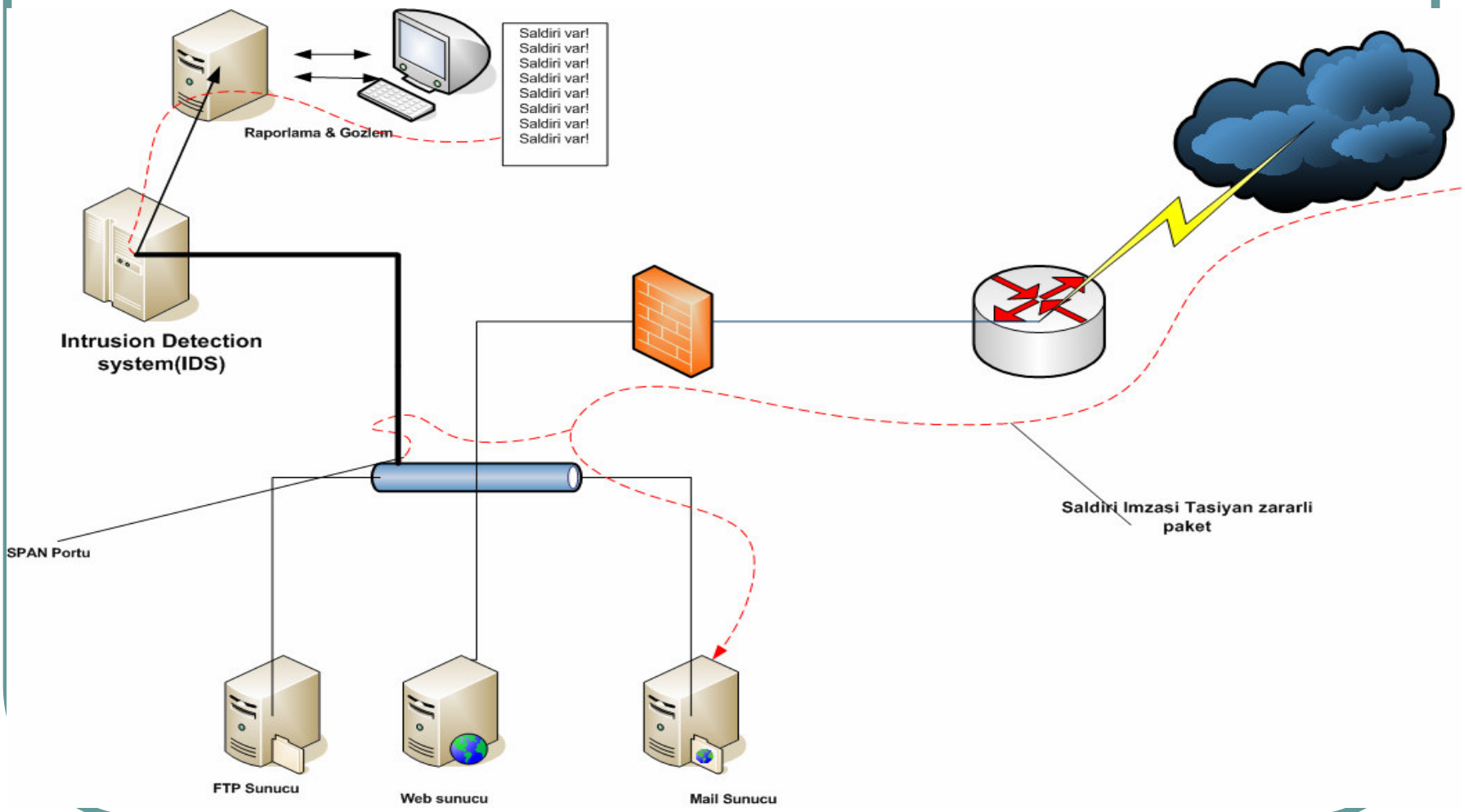
Snort IDS Mimarisi



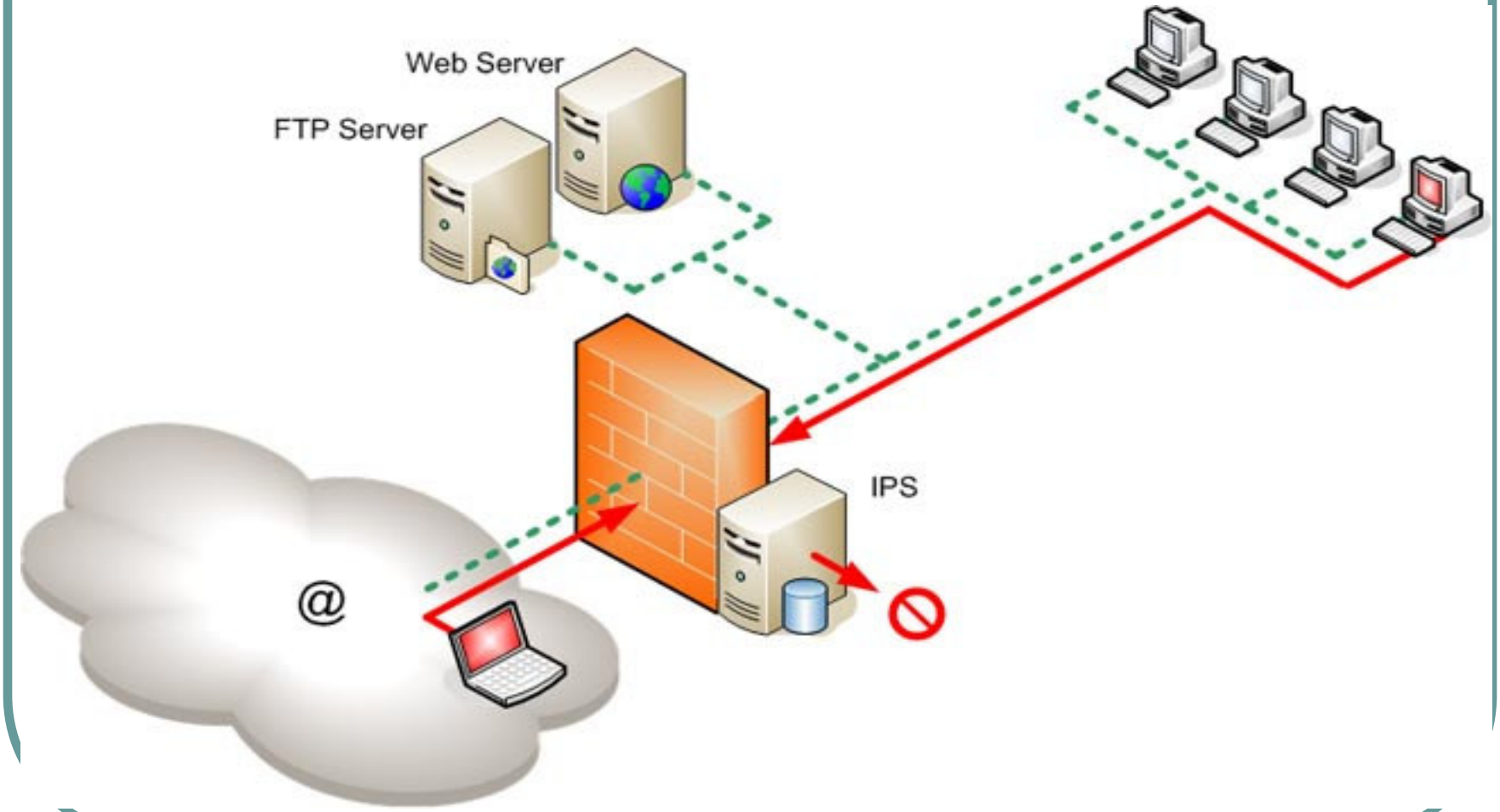
Snort Bileşenleri -Detay

- **Libpcap :** Snort'un Ethernet kartından ham verileri almasına yarayan bileşen.
- **Decoder:** Libpcap'in gönderdiği 2. katman verisini ayrıştırarak(2. katman için Ethernet, 802.11, 3. katman için IP, ICMP ,4. katman için tcp/udp gibi) ve bir üst katmana sunar.
- **Preprocessor:** Çözümlenmiş paketleri Snort'un anlayacağı daha anlamlı parçalar haline getirir. Snort yapılandırma dosyasından aktif edilebilir ya da devre dışı bırakılabilir.. Mesela port tarama pre.'ini aktif hale getirilirse Snort port tarama işlemlerini başarı ile yakalayacaktır.
- **Detection Engine:** Snort'un kalbi olarak da nitelendirilebilecek bu bileşen paket decoder ve prep. bileşenlerinden gelen paketleri detection pluginlerini ve önceden belirlenmiş saldırı imzalarını kullanarak 4. katman ve üzerinde işleme sokar.
- **Output:** Snort tüm bu işlemler sonucu bir uyarı verir ve bu uyarıyı kaydeder. Output plugini bu uyarının nasıl olacağı ve nereye kaydedileceği konusunu yönetir. Çeşitli output pluginler: Mysql, Oracle , syslog , ikili dosya formatı ve text dosyadır

Snort Çalışma Modları -NIDS

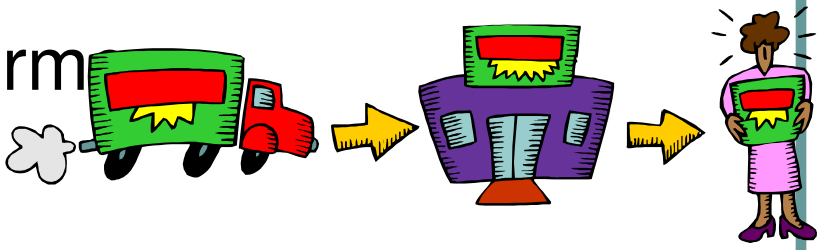


Snort Çalışma Modları -NIPS



Ön işlemciler (Preprocessors)

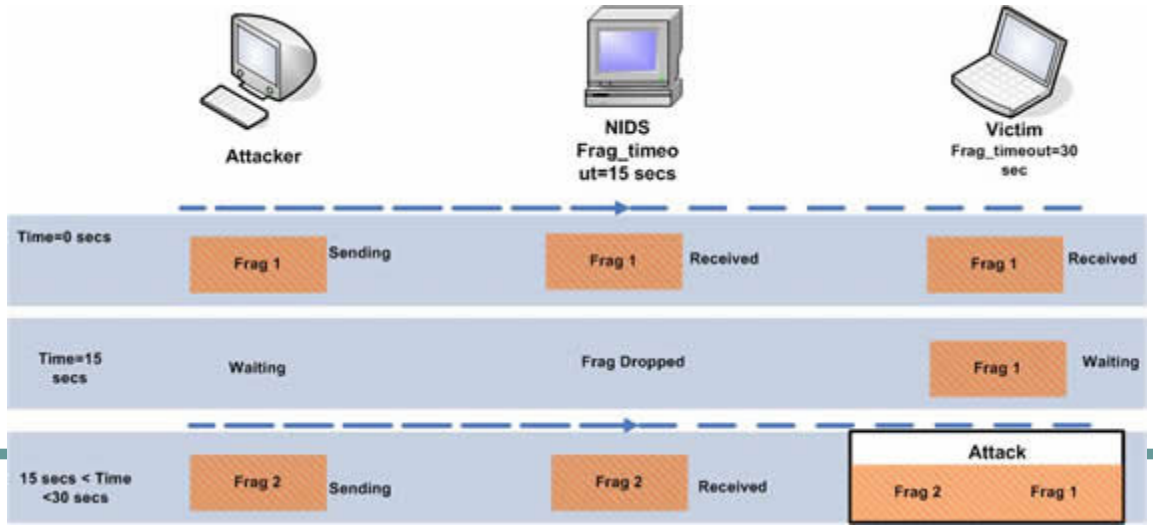
- Packet Decode → **Preprocessors** → Detection Engine
- Amaç: Paket normalleştirme
  - Ip defragmentation
  - Portscan Algılama
  - Web trafik normalleştirme vs
- Temel Kullanımı
  - preprocessor <name>: <options>
- Sık Kullanılan Ön işlemciler: Frag3, Stream4, Portscan, Telnet Decode, HTTP Inspect, SSH, DNS vs



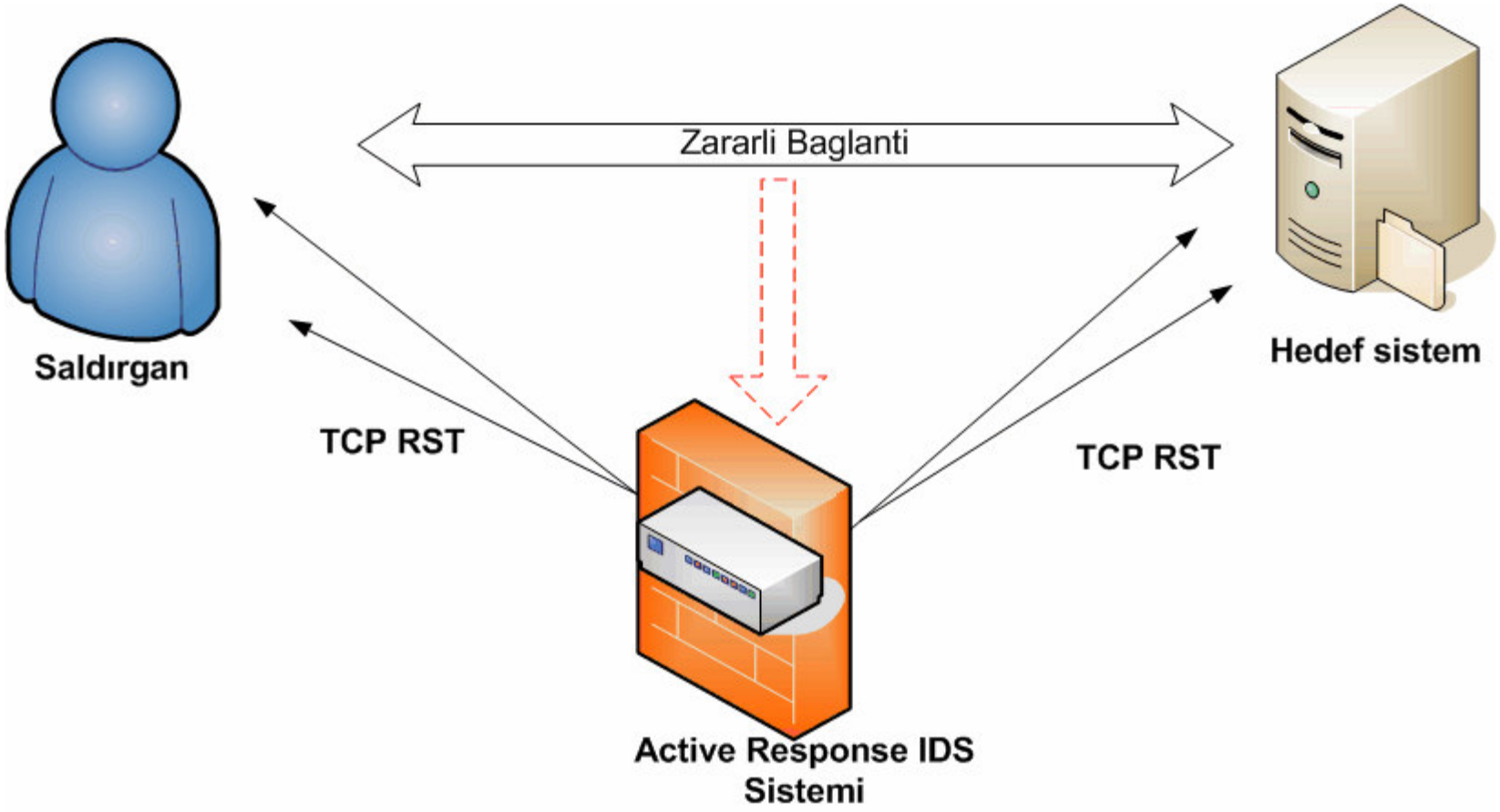
Stream4 &Frag3 Ön işlemcileri

- Stream4 : Tcp Stream Reassembly
- Frag3: Hedef Tabanlı IP Parçalama modulü

```
preprocessor frag3_global: prealloc_nodes 8192
preprocessor frag3_engine: policy linux, bind_to 192.168.1.0/24
preprocessor frag3_engine: policy first, bind_to [10.1.47.0/24,172.16.8.0/24]
preprocessor frag3_engine: policy last, detect_anomalies
```



Aktif Yanıt sistemi Saldırı Bloklama



Flexresp Kullanımı

- Kurulumda --enable-flexresp ile derlenmeli

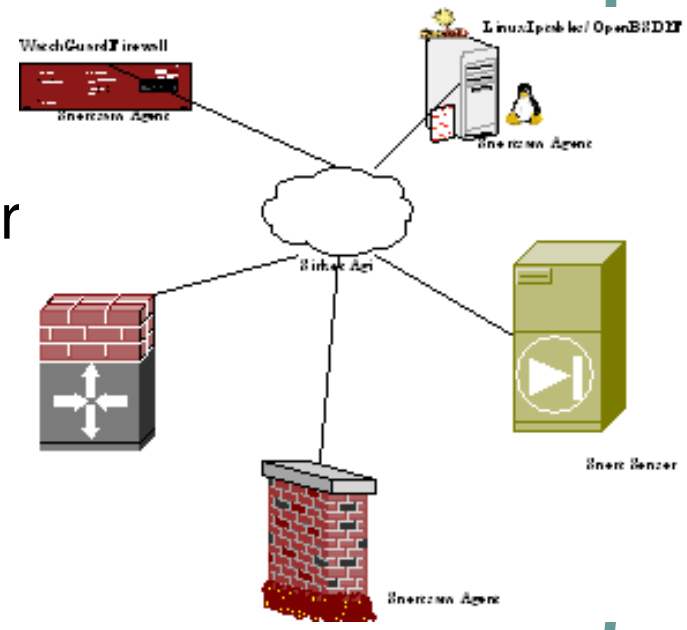
```
 alert tcp $HOME_NET 2401 -> $EXTERNAL_NET any (msg:"MISC CVS invalid repository
response";   flow:from_server,established; content:"error "; content:"\: no such
repository"; content:"I HATE  YOU"; classtype:misc-attack; sid:2009; rev:1;)
```

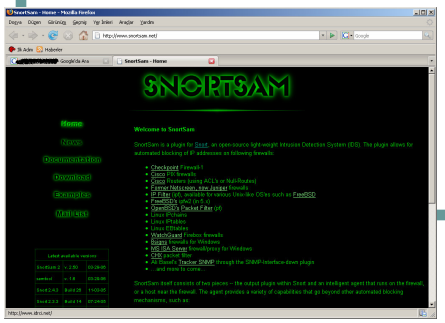
- Dikkatli Kullanılmalı! Dos tehlikesi
- Bloklama Seçenekleri

Option	Description
rst_snd	Send TCP-RST packets to the sending socket
rst_rcv	Send TCP-RST packets to the receiving socket
rst_all	Send TCP_RST packets in both directions
icmp_net	Send a ICMP_NET_UNREACH to the sender
icmp_host	Send a ICMP_HOST_UNREACH to the sender
icmp_port	Send a ICMP_PORT_UNREACH to the sender
icmp_all	Send all above ICMP packets to the sender

SnortSam ile Saldırı Engelleme

- SnortSam -> Snort output plugin + Snortsam Agent
- Active Response Özelliği != IPS
- BeyazListe IP Desteği
- Ajan Snort arası şifreli iletişim
- Olaylar için loglama ve mail ile bildir
- Zamana bağlı bloklama desteği
- Iptables, PF, Cisco Router,
- Checkpoint, Microsoft ISA..





SnortSam ile Bloklama

- Snort.conf
  - output alert_fwsam: firewall/idspassword

alert tcp any any -> $HTTP_SERVERS 80 (msg:"WEB-MISC http directory traversal"; flags: A+; content: "..\\";reference:arachnids,298; **fwsam: dest, 15 minutes;)**

Performans

- Kötü performans=Paket Kaybı=False negatives
- Performansı Etkileyen noktalar
  - Output(çıkış) eklentileri
  - Preprocessors(Önişlemciler)
  - Rules(Kurallar)

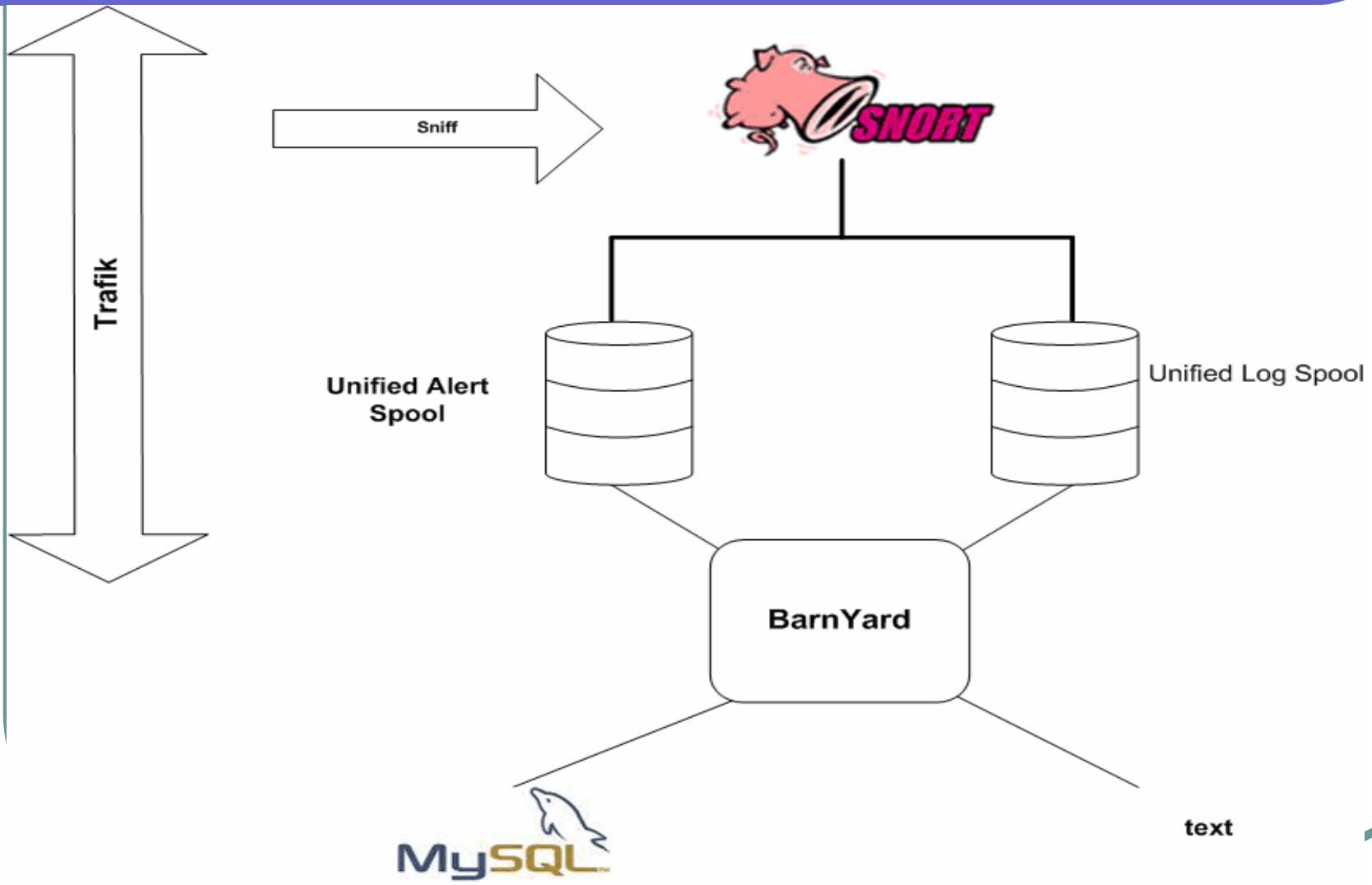
Düşük Performanslı IDS için

- ASCII formatında Loglama
- Önişlemcilerin yanlış/eksik yapılandırılması
- Gereksiz kural fazlalığı
- Kalitesiz(yavaş) donanım kullanımı
- Çıkış plugininin performansı(database, unified)

Yüksek Performanslı IDS için

- Binary(ikili) Loglama formatı seçimi
- Denetlenmiş kural seti
- Gereksiz Önişlemci iptali
  - Ip defragmentasyonu router yapiyorsa ids yapmamali
- Hedef sistemlere uygun kural yazımı!
- Portscan thresholdların düşürülmesi

Unified Output Eklentisi



NIPS Olarak Snort

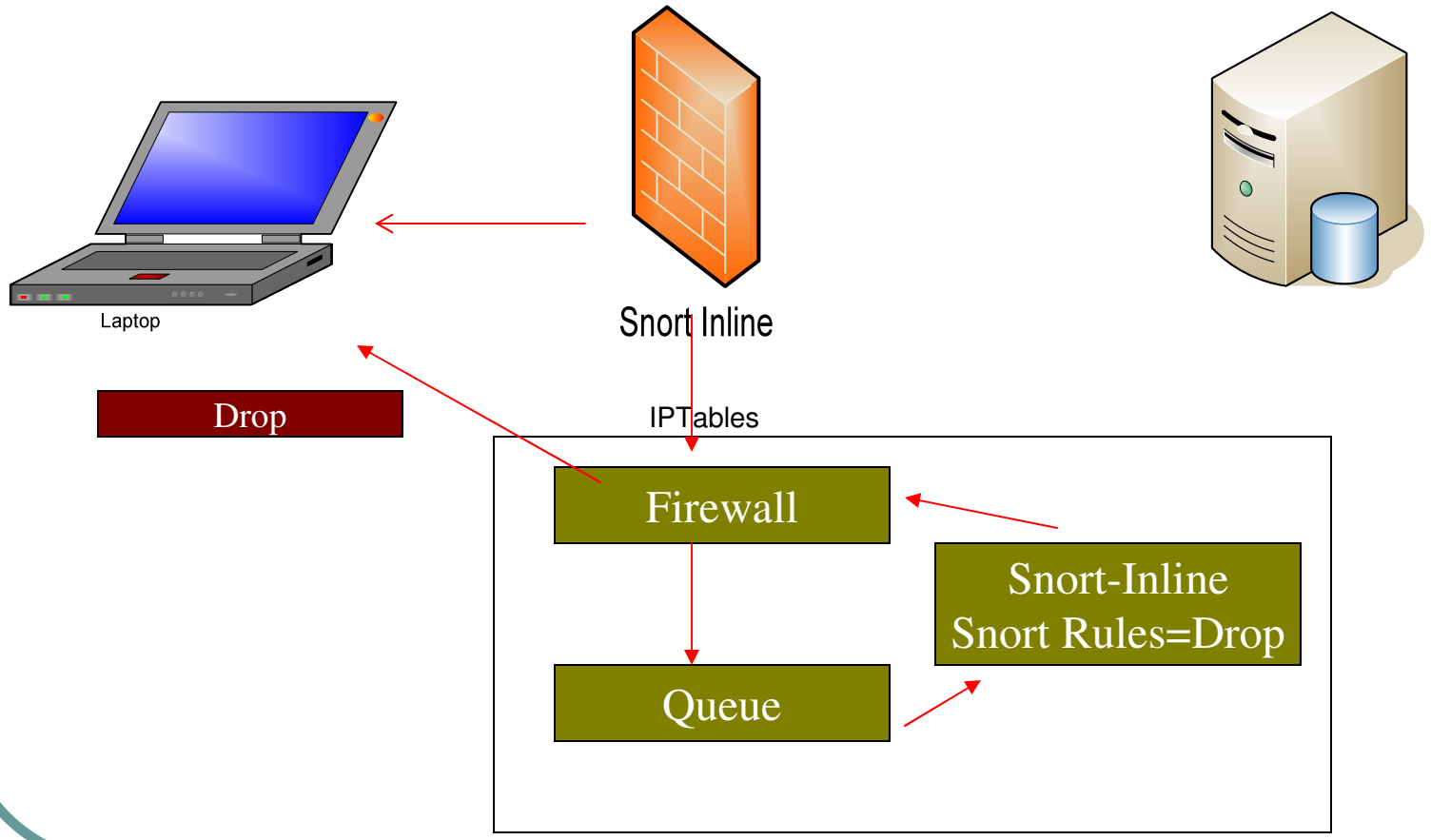
- Ilk olarak Honeynet Projesinde kullanıldı
- 2. Katmanda çalışabilme özelliği
  - Linux/BSD Bridge fonksiyonu
    - #/usr/sbin/brctl addbr br0
    - #/usr/sbin/brctl addif br0 eth0
    - #/usr/sbin/brctl addif br0 eth1
    - #/sbin/ifconfig br0 up
- Saldırı engelleme, antivirus koruması , p2p engelleme, pishing vs amaçlı kullanım
- Linux -> Iptables, Libipq
- freeBSD -> IPFW, Divert Sockets
- OpenBSD -> PQ

Snort_inline

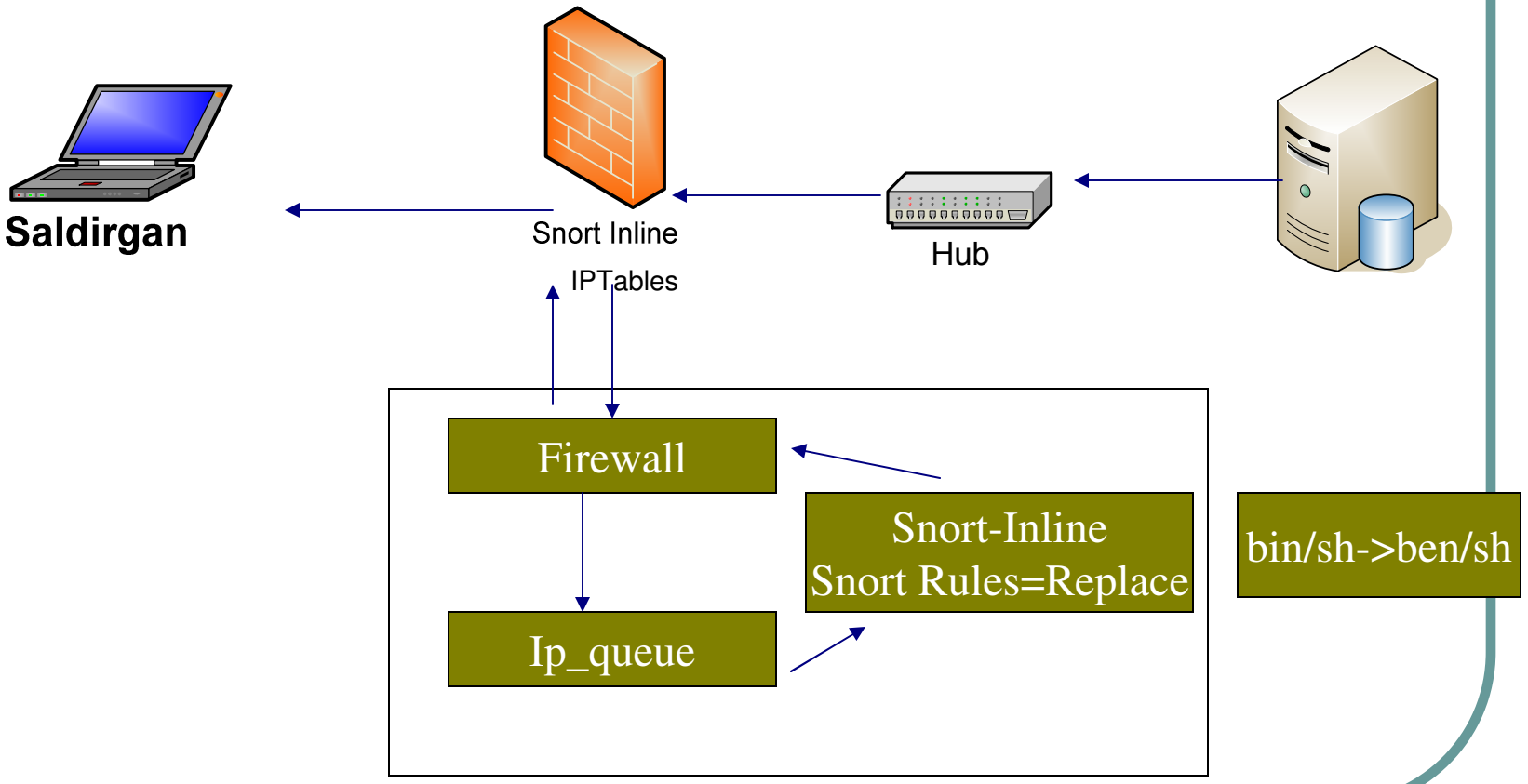
- Kurulum için gereksinimler
  - Iptables, LibIpq desteği için tekrar derlenmeli(make install-devel)
  - Libnet Kurulumu
- Hangi Portlar için devreye alınacak
  - iptables -D INPUT -p tcp --dport 80 -j QUEUE
  - iptables -D INPUT -p tcp --dport 23 -j QUEUE

drop tcp any any -> any 80 (classtype:attempted-user;
msg:"Port 80 connection initiated";)

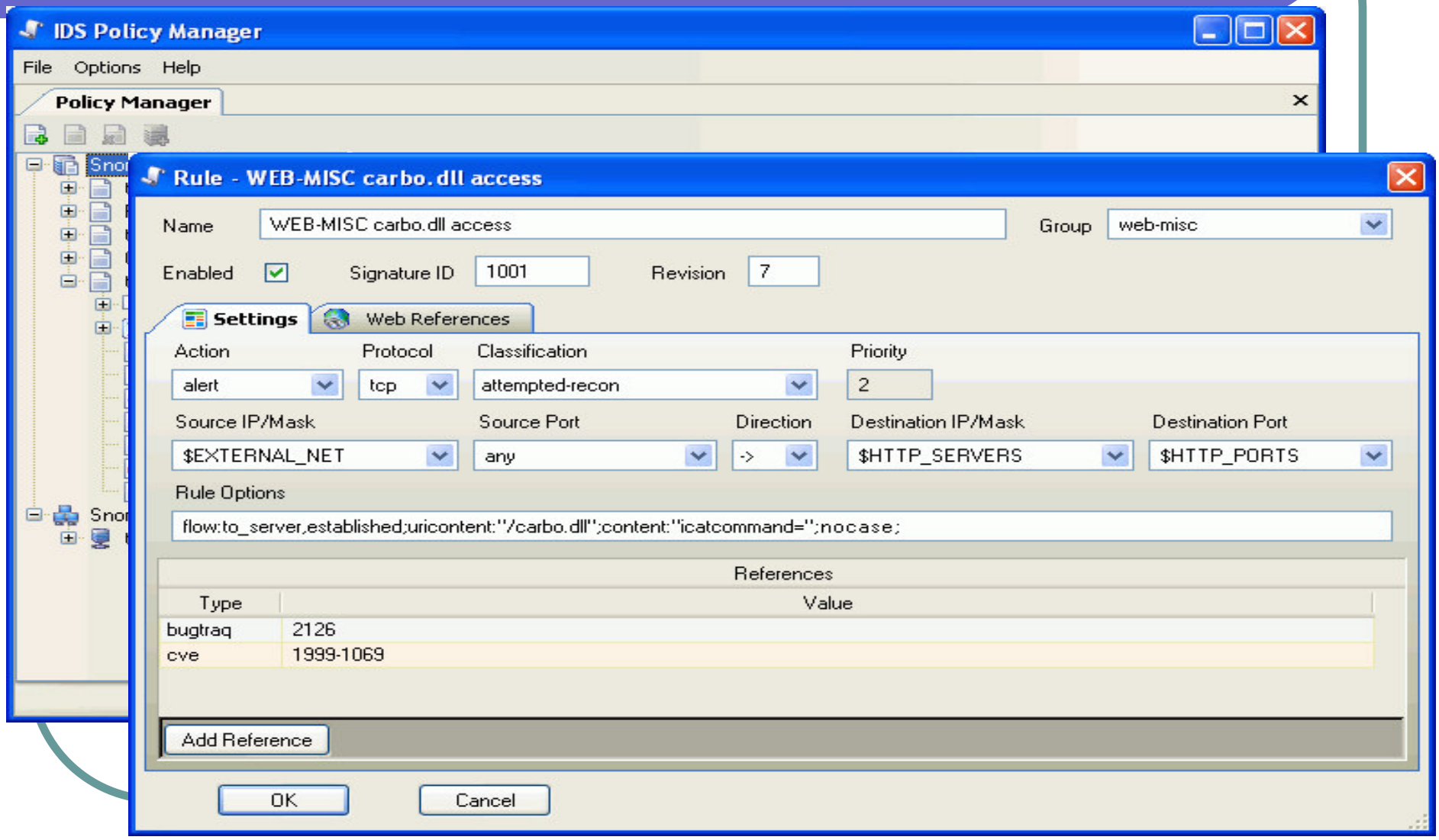
Snort-Inline Drop Mode



Snort-Inline Replace Mode



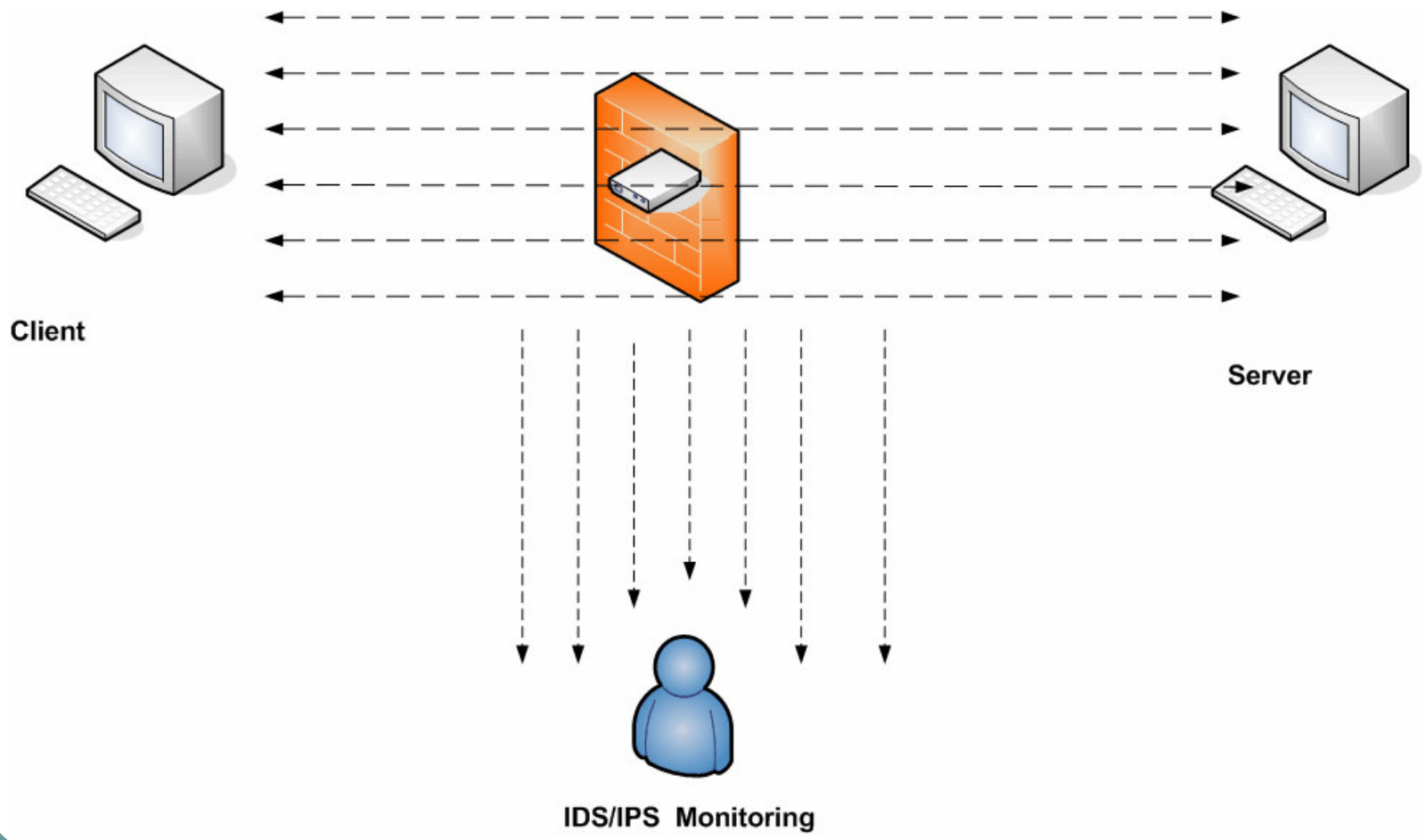
Yönetim Araçları



IDS/IPS Testleri

- IDS/IPS fonksiyonlarını denetleme
  - Performans, kural seti, alarm mekanizması
- Sonuçlar..
  - False positive oranı
  - False negative oranı
- Test Araçları:
  - Fragroute, ftester, Metasploit, Nessus, Nmap, Tomahawk, idswakeup

İstemci-Sunucu IDS Test Yapısı

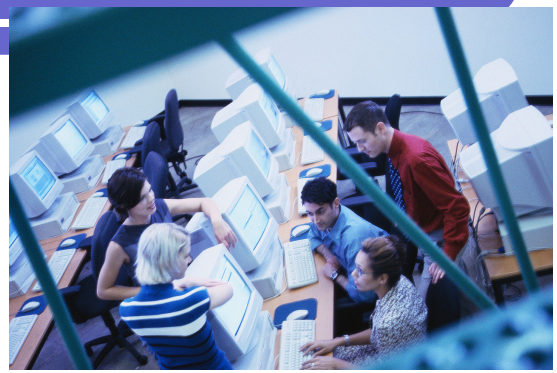


Ftester – IDS Test Aracı

- İstemci-sunucu Mimarisi(ftest- ftestd)
- Firewall Testleri
- IDS Testleri
- IP Fragmentation / IP Spoofing
- IDS Atlatma teknikleri
- Snort Kurallarınu kullanabilme yetenegi

```
ids-conn=192.168.0.10:23:10.1.7.1:1025:PA:TCP:0:to su root
ids-conn=192.168.0.10:1025:10.1.7.1:80:PA:TCP:0:cmd.exe
ids-conn=192.168.0.10:1026:10.1.7.1:80:PA:TCP:0:ftp.exe
insert /etc/snort/exploit.rules 192.168.0.10 10.1.7.1 0
insert-conn /etc/snort/web-misc.rules 192.168.0.10 10.1.7.1 0
```

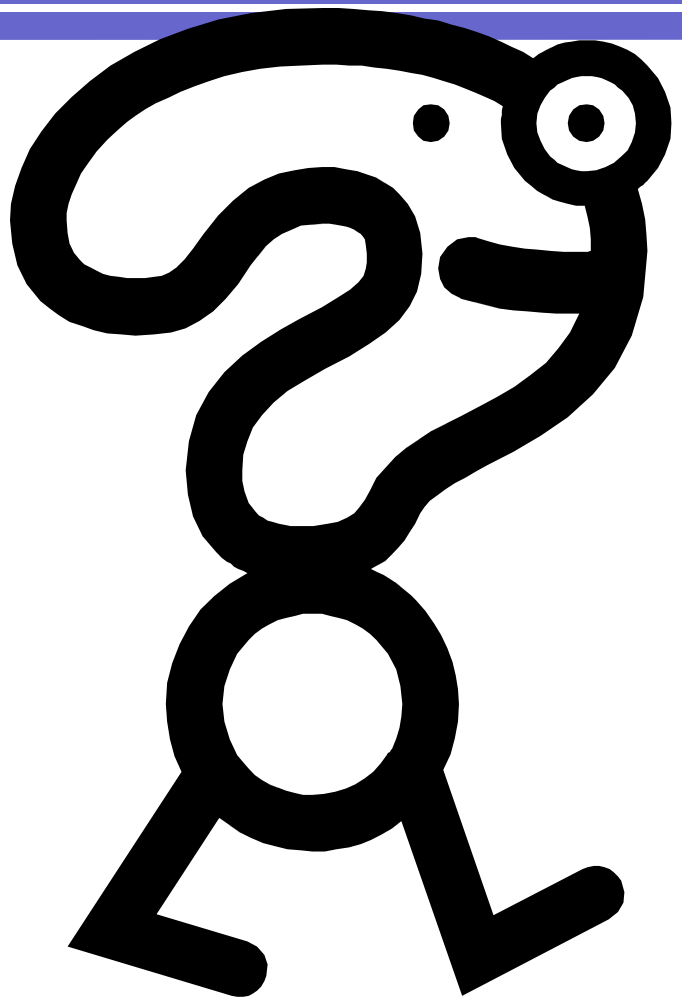
!Sonuc



- Eğitim Şart ;-)
- Türkiye Güvenlik eğitimleri
- Kitap, Belge, Yayinlar..

  Açık Akademi Yayınlari – Güvenlik Kitapları
  - Ağ guvenligi ipuclari
  - TCP/IP Guvenligi
- Olympos Security(www.olympos.org)
- http://netsec.huzeyfe.net – Ağ Güvenliği Listesi

Sorularınız



Teşekkürler..