WWW.BITEL.COM.TR

DERIN PAKET İNCELEME

-Deep Packet Inspection (DPI)-

Teknoloji ve İşlevleri

Bilgin Yazar

11/2009

DPI

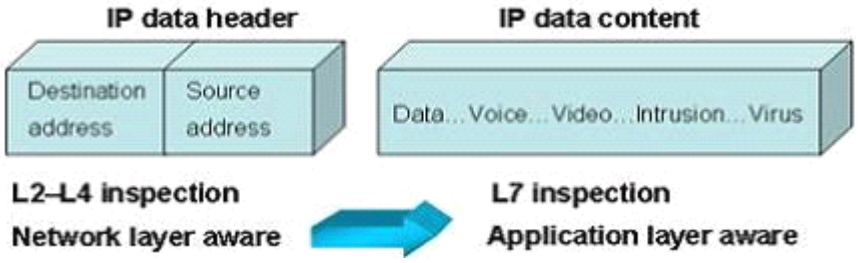
Bilgi alışverişini analiz etmeye çalışan giderek çok önem kazanan yöntemlerden biri de Derin Paket İnceleme denilen İngilizce'de Deep Packet Inspection (DPI) denilen internet bilgi alışverişinin incelenmesi ve takibi. Bu v.b. yöntemler günümüzde internet servis sağlayıcıları, Google/Gmail gibi uygulama sağlayıcılar ve güvenlik güçleri tarafından çeşitli şekillerde kullanılmaya çalışılıyor. Örneğin Gmail kişilerin emaillerini analiz ederek onların yaptıkları email görüşmelerinde geçen kelimelere göre reklam vermeye çalışıyor. Devamında her bir kişi hakkında çok detaylı analizler yapacak duruma geleceğinden, kişileri değişik şekillerde yönlendirecek bir konuma sahip olacak. Güvenlik güçleri ise genel olarak bilgi alışverişinde, örneğin gönderilen emaillerde suç oluşturma ihtimali olabilecek "Bombayı Hazırlıyoruz" gibi kelime, cümle analizleri yapmanın yanında, takip edilen kişi ya da kişilerin bütün bilgi alışverişlerini izlemeye çalışıyorlar.

DERIN PAKET İNCELEME

İÇINDEKILER

DPI'A GIRIŞ

Derin paket inceleme (DPI), genel paket analizinden daha derin incelemedir. Genel paket inceleme sadece kaynak adresi, hedef adresi, kaynak portu, hedef port ve protokol türü de dahil olmak üzere IP paketinin katman 4 ve altındaki katmanların içeriğini analiz eder. DPI ise, uygulama katmanı paketlerindeki tüm uygulamaları ve içeriği analiz eder. Aşağıdaki resimde temel kavram gösterilmektedir. (Huawei-1)



Teknoloji Teorisi

Ağ içindeki çok çeşitli uygulamaları verimli bir şekilde belirlemek DPI teknolojisinde anahtar cümledir.

Genel Paket İnceleme teknolojisi ağ bağlantı noktası (port) numarası üzerinden uygulama türlerini belirler. Örneğin, 80 port numarası tespit edildiğinde bilinir ki bu standart bir uygulamadır. (Huawei-1)

Common TCP/IP Port Numbers	
Port Number	**Application**
Port 21	FTP File Transfer
Port 25	SMTP E-mail Delivery
Port 80	HTTP - Internet Traffic
Port 110	POP3 Mail Delivery and Collection
Port 143	Remote E-mail Access (IMAP4)

Ancak kötü amaçlı uygulamalar gizli ya da sahte port numaralarını kullanarak paket incelemede tesbit edilmeyerek ağa girebilirler. Geleneksel L2-L4 incelemesiyle bu tür kötü amaçlı uygulamaları tesbit edilemez. DPI paket içeriğini inceleyerek kötü amaçlı uygulamaları tesbit eder. (Huawei-1)

DPI inceleme teknolojileri şu şekilde sınıflandırılabilir:

(1) İmza Tabanlı İnceleme – Tanıma

Farklı uygulamalar farklı protokoller kullanırlar. Farklı protokoller kendine has parmak izi ya da imza diyebileceğimiz bilgiler içerirler. Bu parmak izi bilgileri port, harf-kelime (string) ya da bit dizisi olabilir. İmza tabanlı incelemelerde veri transferi - akışı sırasındaki paketlerdeki parmak izlerine bakılır. Böylece DPI, veri akışındaki uygulamaları tesbit eder.

İnceleme- tanıma modlarına göre imza tabanlı tanıma teknolojisi üç şekilde sınıflandırılabilir:

- Sabit konuma göre imza eşleme
- Fluctuant- değişken konuma göre imza eşleme
- Durum bazlı imza eşleme

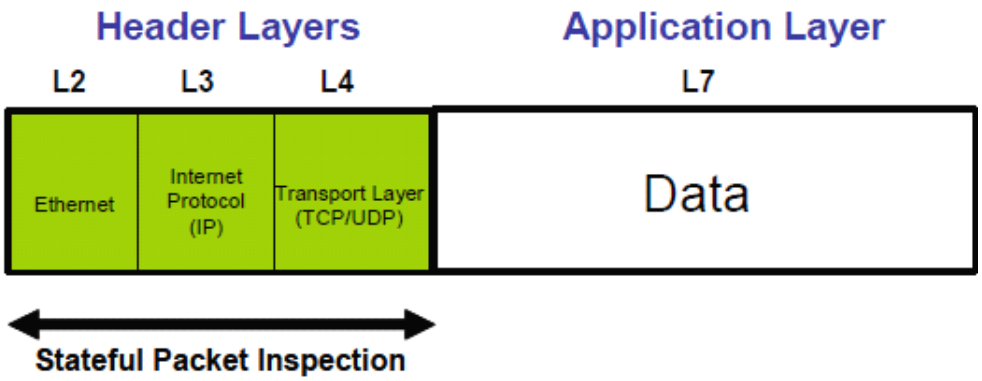


Figure – Ethernet frame and how Stateful Packet Inspection (SPI) views it

(Esoft-1)

Parmak izi kapsamındaki bilgiler artırılarak, imza tabanlı inceleme kendi işlevlerine esnek bir şekilde genişletebilir ve yeni protokolleri algılayabilir.

Örneğin büyük dosyaların indirmek için kullanılan Bittorrent protokolünün tanınması ters mühendislik yöntemi ile peer protokolünün analizi ile gerçekleştirilir. Peer protokolü peer (eş) ler arasında bilgi alış-verişi sağlar. Peer protokolü handshake olarak bilinen el sıkışma ile başlar ve yuvarlak mesaj akışı (circular message flow) ile devam eder. Her bir mesajdan önce mesaj uzunluğunu gösteren bir numara bulunur. Handshake sırasında 19 alan(field)lık bir bilgi BitTorrent protokolüne ait string ile birlikte gönderilir. Bu 19BitTorrent Protokol stringine Bitrorrent in parmak izi ya da imzası denir.(Huawei-1)

(2) Uygulama katmanı ağ geçidi tabanlı inceleme

Kontrol akışı (control flow) ve bazı hizmetlerin hizmet akışını (service flow) birbirinden ayırmak gerekir. Ancak hizmet akışının ayırt edici hiçbir özelliği bulunmaz. Bundan dolayı, hizmet akışını incelemek için uygulama katmanı ağ geçidi tabanlı inceleme gerekli olur.

Uygulama katmanı ağ geçidi kontrol akışını ilk başta belirler ve kontrol akışının protokolünü çözümler (parse). Daha sonra, ağ geçidi hizmet akışını incelemeye başlar.

Her bir protokol farklı uygulama ağ geçitleri tarafından analiz edilmelidir.

Örneğin SIP ve H323 protokollerini ele alalım. RTP formatındaki ses akışında olduğu gibi, SIP ve H323 sinyal alış-verişi yaparak veri kanalı ile haberleşmeye başlarlar. Ancak RTP akışını kuran protokol RTP akışı incelenerek anlaşılamaz. Protokol sadece SIP ve H323 arasındaki sinyal değişiminin incelenmesiyle analiz edilebilir. (Huawei-1)

(3) Davranış-tabanlı inceleme

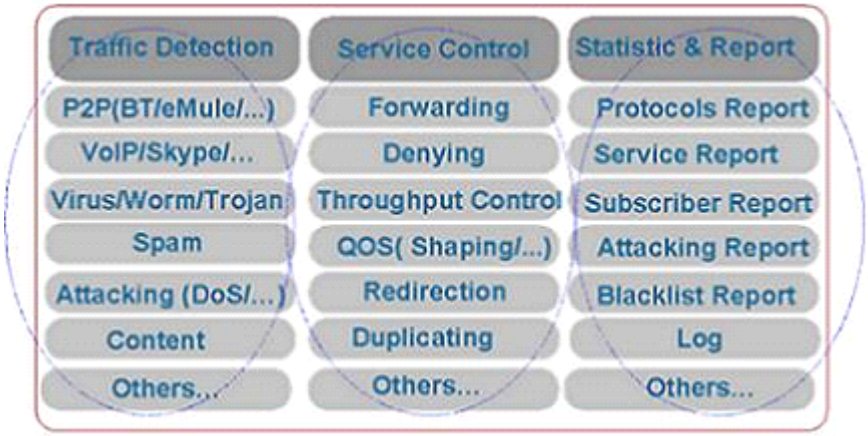
DPI, kullanıcı terminallerinin geçmiş - eski veri akışlarını inceleyerek kullanıcının yapmakta olduğu ya da yapacağı davranışlar hakkında karar verebilir. Bu tür inceleme veri akışı protokole göre tanımlanamadığında yapılabilmektedir. Yani protokole göre tesbit edilemeyen hizmetler için kullanılmaktadır.

Örneğin, içeriği bakımından SPAM veri akışını normal email veri akışından ayrıştırmak mümkün değildir. SPAM veri akışı kullanıcı davranışları incelenerek tanımlanmaktadır.

Yukarıdaki 3 inceleme tekniği çeşitli protokoller için kullanılmakta ve birbirinin yerine kullanılamayacağı anlaşılmaktadır. (Huawei-1).

DPI Uygulamaları

DPI sistemi IP ağı içine konuşlandırarak servis tesbiti (algılama), servis kontrolü ve servis istatistikleri gerçekleştirilebilir.



Servis Algılama

Servisleri algılamak için iki yöntem vardır:

- Taşıyıcı (carrier) tarafından aktif edilen yasal servisleri algılama
- Taşıyıcı tarafından izlenen servisleri algılama

Birinci yöntemde servis akışının beş katı incelenebilir. Örneğin VOD servis akışının IP adresi VOD sunucusunun ağ sekmentine aittir. Sistem servisi ACL (Asynchronous Connectionless) mod a göre tanımlamaktadır.

İkincisi DPI teknolojisini kullanır ve servis akışının türünü ise birinci yönteme göre belirler:

IP veri paketinin içeriği analiz edilir

- İmza- parmak izi tesbit edilir
- Servisin ilgili davranışlarına yönelik istatistik oluşturulur.

Servis İstatistikleri

DPI hizmet istatistiklerinin işlevleri şunlardır:

- Servis akışının ağ üzerinde dağıtımı ve servis kullanımı ile ilgili açık bir fikre sahip olmak (Bu sayede taşıyıcı hızlı bir şekilde kim ya da hangi servisler ağ-şebeke faaliyetlerini etkilemektedir belirleyebilir)
    - Ağ-şebeke faaliyetlerini etkileyen faktörlerin tesbiti
    - Ağ ve servislerin optimizasyonu için gerekli verilerin belirlenmesi

Örneğin servis analizi aşağıdakileri yapabilir:

- Cazip-çekici servislerin belirlenmesi
- Servislerin SLA(service level agreement) gereksinimlerini karşılayıp karşılamadıklarının kontrolü
- Saldırı akışının yüzdesinin -istatistiğinin belirlenmesi
- Oyun servislerinden yararlanan kullanıcıların istatistiğinin belirlenmesi
- Bant genişliğini çok fazla işgal eden servislerin istatistiğinin belirlenmesi
- Illegal VOIP kullanan kullanıcıların istatistiğinin belirlenmesi

Servis Denetimi - Kontrolü

Servis akışları belirledikten sonra, DPI servis akışını tarih, trafik kullanıcı, zaman, bant genişliği gibi ağ yapılandırma durumlarına bağlı olarak denetler. Kullanılan yöntemler yönlendirme, engelleme, bant genişliği sınırlama, şekillendirme ve öncelikleri belirleme şeklinde ifade edilebilir.

Servis faaliyetlerinin düzeni için, servis kontrol politikaları poliçe sunucusunda düzgün bir şekilde yapılandırılmış olmalı ve kullanıcı çevrimiçi (online) olduğunda gönderilebilmelidir. (Huawei-1)

DPI Alanındaki Gelişmeler

DPI teknolojisi Anti-denetim teknolojisi ile çatışmaktadır. DPI teknolojisi gelişirken aynı zamanda veri şifreleme, gizli imza ve tünel teknolojisi ile ducking inceleme de gelişmektedir. Mevcut DPI teknolojisinin daha kapsamlı incelemeler yapabilmesi için bu gelişmelere adapte olması gerekmektedir.

Gelecekte, DPI teknoloji yaygın güvenlik ve hizmet kontrolü alanlarında uygulanacaktır. DPI, taşıyıcıya (carrier) şebekenin (ağ) daha ayrıntılı kontrolü ve düzenlenmesinde yardımcı olacaktır. (Huawei-1)

DPI'ın Karşı Karşıya Olduğu Sorunlar

Nispeten genç bir pazar olarak, DPI endüstrisinin karşı karşıya olduğu bir dizi sorun bulunmaktadır. Örneğin: Standart Benchmark olmaması bir sorundur. Bugün DPI pazarı uygulamaya özel performans bilgilerini içeren kafa karıştırıcı bilgilerle doludur.

Endüstride bağlantı kurulum zamanı, TCP, UDP ve forward throughput testleri gibi standart kriterler (benchmark) gerekmektedir. Bu benchmark bilgileri rakip ürünlerin karşılaştırılabilir performans ölçütleri için gereklidir.

Patentli çözümler mevcut potansiyeli kısıtlamaktadır. Farklı DPI teknolojileri ortaya çıkmakta ve açık mimariye yönelik istekler gündeme gelmektedir. OpenDPI hareketi 3nçü parti geliştiricilerin mevcut ticari çözümler üzerine DPI uygulamaları geliştirmelerine olanak sağlıyacaktır. (Forrester-1)

DPI GEREKSINIMLERI

Yetenek Gereksinimleri

- **Paket Payloadlarını bütün katmanlarda –layerlarda- tarama :** Network Trafiğini izlemek ve kontrol etmek icin DPI'ın gerektiğinde ilk bit ten son bite kadar tarayabilmesi gerekmektedir.

- **Uygulama Sınıflandırılması, Ölçüm ve Raporlama :** DPI performans ölçümü, uygulamaları sınıflamak ve raporlar oluşturmak için gereklidir. Bu sayede network yöneticileri stratejik trafik planlama, policy tabanlı ücretlendirme v.b. yapabilirler.

- **Trafiği Kontrol Edebilmek İçin Politikaların(Policy) Tanımlanması:** Paket Payload taramasına göre uygulama sınıflandırma ve trafiği yönetebilmek için gerekli policy kümesi sayesinde trafikte önceliklendirme ve kontrol yapılabilmektedir. Bu fonksiyon katmanlı servisler ve uygulama denetimi için temel bir özelliktir.

- **Oturum (Session) Belirleme :** DPI gerçek zamanlı katman 2 den katman 7 ye kadar oturum davranışlarını analiz etme, gerektiğinde oturum durum değişimini takip etme ve bireysel kullanıcıların deneyim kalitesi (quality of experience), uçtan uca Anahtar Performans Göstergelerini izleme yeteneğine sahip olmalıdır.

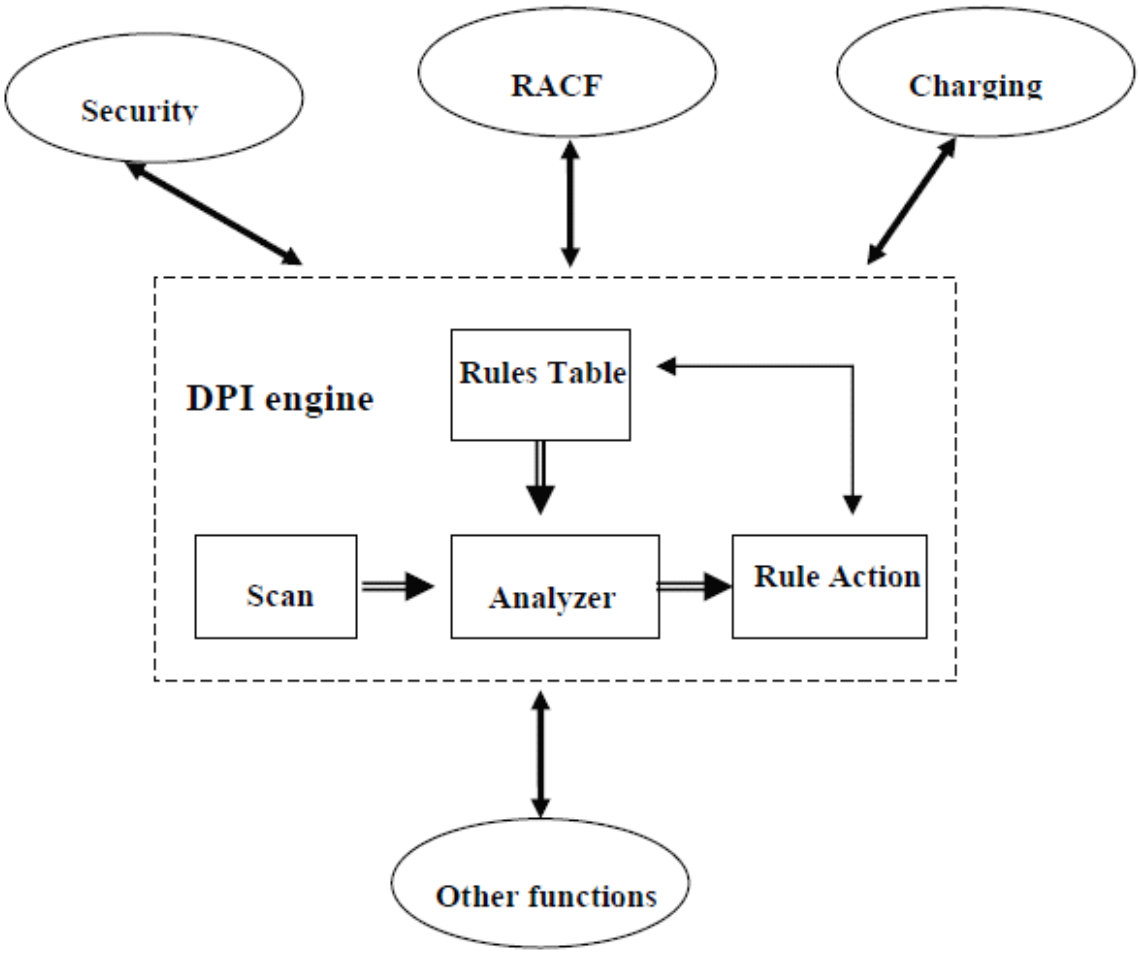
- **Paket Zarflarının (Envelope) Modifikasyonu :** İsteğe bağlı olarak DPI yeni hizmetler sağlamak ve saldırıları önlemek amacıyla paket zarflarında değişiklik yapabilir. Bu isteğe bağlı özellik ile paket işlemeden yeterli granül yapıda ve maksimum esneklikle konfigure edeilebilir ve programlanabilir olmalıdır.

• **Paket Paylod İçeriğinin Modifikasyonu:** DPI paket payload içeriğini değiştirebilecek mekanizmaları desteklemelidir. Dinamik paket ve oturum izlenmesine dayalı olarak, DPI paket içerik modifikasyonu viruslerin temizlenmesi gibi fonksiyonları yerine getirebilir.

• **Paketlerin Oluşturulması:** Network yöneticisine gönderilmek üzere uygun içerik ve zarfı bilgileri ile birlikte paketleri oluşturacak mekanizmaları desteklemelidir. (Y.dpireq -1)

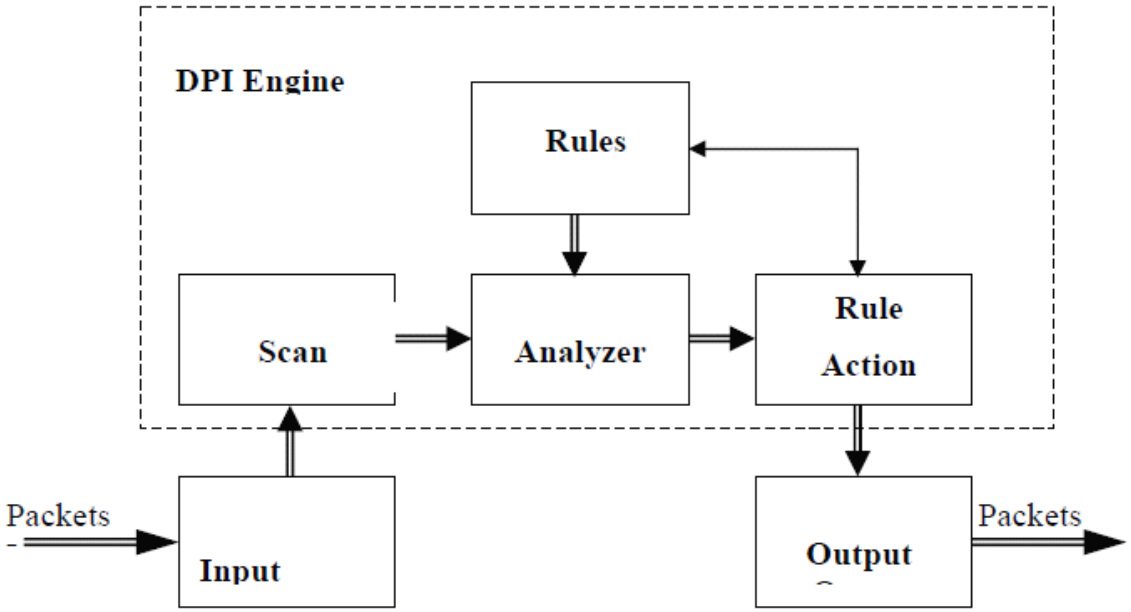
Fonksiyonel Gereksinimleri

Aşağıdaki şekil paket tabanlı network ve NGN ortamında DPI ve diğer bileşenler arasındaki ilişkileri göstermektedir. (Y.dpireq -1)



DPI'ın Mimari Çerçevesi

DPI temel işlevi ve mimari aşağıda şekilde gösterilmiştir.

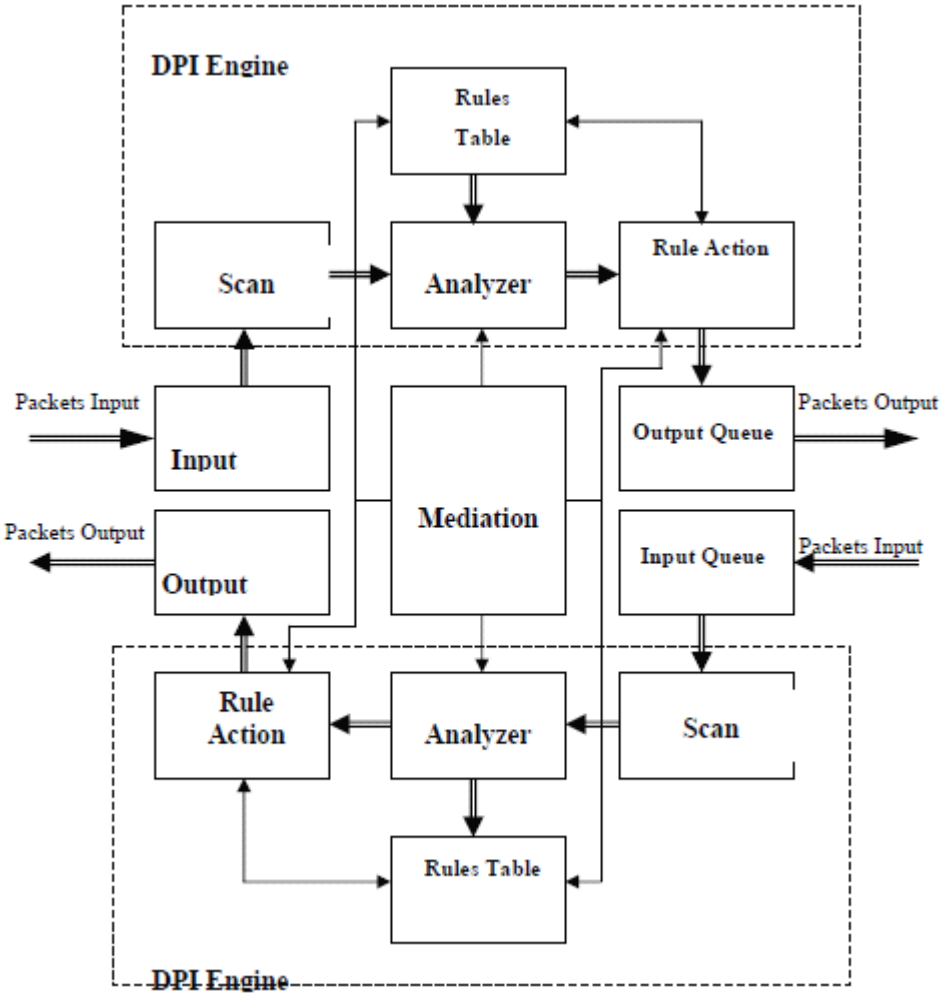


Kurallar (Rules) aşağıdaki kapsamda uygulanmaktadır.

- Trafik sınıflandırma, ölçme, raporlama ve yönetim
- Kaynak yönetimi, giriş kontrolü ve filtreleme
- Poliçe tabanlı engelleme, önceliklendirme, şekillendirme ve zamanlama
- Dinamik kural oluşturulması ve modifikasyonu

DPI en önemli özelliklerinden biri gerçek zamanlı trafik yönetimi yapabilmesidir. Örneğin bir kural uygulandığında bir eşleşme olduğunda ilgili içerik bloka edilebilir ve alarm mesajı oluşturulur ya da ilgili içerik değiştirilir ve yeni bir aksiyon oluşur. Kurallar tablosu bir çok kural elemanını içerir. Farklı katmanlara göre (L2-L7 ve içerik) tanımlanabilir, sınıflandırılabilir ve taşıyıcı gereksinimlerini karşılayacak farklı fonksiyonlara sahip olabilir. DPI engine işlem yaptıktan sonra paketler network e tekrar salıverilir. (Y.dpireq -1)

Aşağıdaki şekil iki yönlü DPI fonksiyon ve mimarisini göstermektedir. Arabuluculuk Birimi (Mediation Unit) iki yönli DPI sağlayabilmek için konuşlandırılmıştır. (Y.dpireq -1)



DPI UYGULAMALARı

DPI'ın kullanım alanları aşağıdaki şekilde açıklanmaktadır: (dpacket-1)

Uygulama	**Açıklama**
Güvenlik	DPI giderek spamla mücadele, phishing, dağıtık denial of service (DDoS) saldırıları, botnets, virüsler ve diğer tehditler konusunda güvenlik uygulamalarına yardımcı olmaktadır.
Yasal dinleme - lawful intercept-	ABD'de The Communications Assistance for Law Enforcement Act (CALEA) - İletişim Yardım Kanunu Uygulama Yasası- ve diğer ülkelerde benzer kanunlar operatörlerin güvenlik hizmetlerinin gözetimi için gerekli ekipmanları kullanmasını gerektiriyor. DPI ise VOIP ortamında yasal dinleme için gereklidir.

Trafik İzleme	DPI kökeni itibariyle, trafik izleme amaçlı olarak operatörlere ağlarında neler oluyor, hangi uygulamalar ne kadar bant genişliği kullanıyor gibi konularda yardımcı olmaktadır.
Trafik Yönetimi	Operatörlerin bir sonraki arzusu DPI'ı kullanarak makro ya da uygulama düzeyinde trafiği kısıtlamak, bloke etmek ve düzenlemek olmuştur. Bu sayede bant genişliğini sömüren P2P gibi uygulamaların etkisini kontrol edebiliyorlar.
Internet Trafiği Paylaşımı (Peering) Kontrolü	Trafik yönetimin bir uzantısı olarak, paylaşım noktalarından oluşan trafiği daha iyi kontrol ederek taşıyıcılara daha fazla kontrol imkanı sağlamaktadır. Internet trafiğinin paylaşımının maliyetini azaltmak her zaman operatörler tarafından arzu edilmektedir.
QoS (Hizmet Kalitesi) Güvencesi	Paket nedir, nereden gelip nereye gitmektedir gibi bilgilere dayalı olarak paket düzeyinde etiketleme ve önceliklendirme sayesinde, DPI farklı uygulamalar için uygulama, hizmet ve müşteri bazında Hizmet Kalitesi Güvencesi için kullanılmaktadır.
Katmanlı Hizmetlerin Provizyonu - Provision of Tiered Services	Eğer granüllü düzeyde QoS yönetebilirsiniz, bir sonraki mantıklı adım, katmanlı servisler sunan operatörler tarafından bu yeteniği paraya dönüştürmektir.
Özelleştirilmiş Fiyatlandırma & Faturalandırma	Uygulama tabanlı fiyatlandırma paketleri ile müşteri hizmetlerinin provizyonu. Örneğin müşterilere oyuna özgü network trafiği sunarak bu tür hizmetlere abone olmaları sağlanabilir.
Olay Tabanlı Faturalandırma ve İzlenebilirlik	Paketlerin hangi tür veri akışına ait oludğunu bilmek ne kadar veri akışı olacak ve bu akış nasıl faturalandırılacak anlamak açısından önemlidir. Örneğin servis sağlayıcıların online mağazalarından müşteriler büyük hacimli video (film gibi) alırlarsa ve indirirlerse, oluşacak trafiğin normal trafik gibi değerlendirerek müşteri aleyhine olması arzu edilmez.
İçerik Zenginleştirme	Paket header ına veri ekleyerek veri akışlarının nasıl davranılacağı ya da bazı durumlarda ne tür veri akışları gönderilecek gibi kararlar verilmesi için gerekli olabilir. Operatörler bunu kullanarak alıcı cihazın (cep telefonu, pc v.b.) yeteneklerine bağlı olarak içeriği değiştirmek

	isteyebilirler.
Reklam	Bu konuda düzenleyici ve kamuoyu bilincini artırıcı çok şey vardır. Reklamın genel kabul görebilecek şekilde sunulabilmesi, müşterilerin reklamlar karşılığında daha ucuz hizmet almasıyla mümkün olabilir.
Reklam Takip	Bu uygulama online reklamların etkisini izleyerek ne ölçüde pazarlama kampanyaları online davranışdan etkilenmektedir belirlemeye çalışır.
Ebeveyn ve Ağ Bazlı Kontrol	Birçok ebeveyn kontrol çözümleri içerik filtrelemede daha fazla imkan sağlamak amacıyla DPI ile çözüm sunmaktadır. Ağ tabanlı uzantı sayesinde istenmeyen URL'ler ya da web sayfaları ebeveyn kontrolü olup olmadığına bakılmaksızın engellenebilir.
Dijital Haklar Yönetimi (DRM)	Bazı ülkelerde, yasal çerçeveler etkin DRM uygulamasını sağlamak için DPI kullanımını mecbur edecek bir ortam oluşturmaktadır. Bu sayede içeriğin kopyalandığının analizi filtrelemeyi mümkün kılarak yapılabilir.
Özelleştirilebilir Yönetilebilen Müşteri Servisleri	DPI'ın yetenekleri operatörleri de aşabilir. Örneğin yeni çözümler internet servis sağlayıcılara (ISP) özelleştirilebilir DPI tabanlı çözümleri uç kullanıcılara sunabilmektedir. Ayrıca kurumsal müşterilere IP-VPN trafiğini DPI tabanlı portaller aracılığıyla daha iyi gözlemlemeleri için servislerde sunulmaktadır.

DPI PAZAR TAHMINI - 2009

• DPI ürünlerinin Dünya çapında gelirleri 2012 yılına kadar 1 milyar dolara ulaşması bekleniyor.

• Üreticiler hizmet farklılaşması ve gelir artışı için bir motor olarak DPI'ının yeni çeşit ürün konumlandırması yapıyorlar.

• Servis sağlayıcılar hala kendi ağlarındaki istenmeyen trafiği yönetmek istiyorlar. Bu mobil operatörler için yeni bir konu durumundadır.

• Mobil operatörler mobil veri servisleri daha kritik hale geleceği için önümüzdeki beş yıl içinde DPI pazarının büyümesini sağlayacaklardır. (dpacket-1)

AÇıK KAYNAK KODLU DPI

Ipoque firmasi açık kaynak kodlu DPI uygulamasını OpenDPI.org da yayınladı. OpenDPI motoru, LGPL lisansı ile kullanılabiliyor ve ipoque'un ticari yüksek performanslı ve fiyatlı donanımı da içeren DPI tarama motorundan oldukça farklı. Açık kaynak kodlu uygulama ticari uygulamaya göre yavaş ve şifreli veri alışverişine yönelik DPI fonksiyonlarını içermiyor. (opensource-1)

Şirketin bu şekilde bir girişimde bulunmasının nedenini ise ipoque CEO'su Klaus Mochalski müşterilere DPI konusunda şeffaflık sağlamak olarak açıklıyor. (opensource-1)

OpenDPI motoru şifreli olmayan çok sayıda protokolü inceleyebiliyor: (opensource-1)

- **P2P dosya paylaşımı:** BitTorrent, eDonkey, Kazaa / FastTrack, Gnutella, WinMX, DirectConnect, appleJuice, Soulseek, XDCC, Filetopia, Manolito, iMesh, Pando
- **Voice over IP:** SIP, IAX, RTP
- **Anlık Mesajlaşma:** Yahoo, Oscar, IRC, Jabber, Gadu şifresiz! Gadu, MSN
- **Akış Protokolleri:** ORB, RTSP, Flash, MMS, MPEG, Quicktime, Joost, WindowsMedia, RealMedia, TVAnts, SopCast, TVUPlayer, PPStream, PPLive, QQLive, Zattoo, VeohTV, AVI, Feidian, Ececast, Kontiki,,, RTSP Taşı SCTP, SHOUTcast
- **Tünel Protokolleri:** IPSec, GRE, SSL, SSH, IP IP
- **Standart Protokoller:** HTTP, Direkt indirme bağlantıları (1-click file Hosters), POP, SMTP, IMAP, FTP, BGP, DHCP, DNS, EGP, ICMP, IGMP, MySQL, NFS, NTP, OSPF, pcAnywhere, PostgresSQL, RDP SMB, SNMP, SSDP, STUN, Telnet, Usenet, VNC, IPP, mDNS, NetBIOS, XDMCP, RADIUS, syslog, LDAP
- **Oyun Protokoller:** World of Warcraft, Half-Life, Buhar, Xbox, Quake, Second Life

Ipoque açık kaynak kodlu uygulamada kendi DPI ürünlerinin trafik içeriğine bakmadığına ya da saklamadığına insanları ikna etmek istiyor. Örnek olarak Second Life Protokolunun http://wiki.secondlife.com/wiki/Protocol incelenmesi aşağıdaki şekildedir: (opensource-1)

>if ((**ntohs(packet->udp->dest) == 12035** || **ntohs(packet->udp->dest) == 12036** || **(ntohs(packet->udp->dest) >= 13000** && **ntohs(packet->udp->dest) <= 13050**)) //port

&& **packet->payload_packet_len > 6** // min length with no extra header, high frequency and 1 byte message body

&& **get_u8(packet->payload, 0) == 0x40** // reliable packet

&& **ntohl(get_u32(packet->payload, 1)) == 0x00000001** // sequence number equals 1

//**ntohl (get_u32 (packet->payload, 5)) == 0x00FFFF00** // no extra header, low frequency message - can't use, message may have higher frequency

```
) {

IPQ_LOG(IPOQUE_PROTOCOL_SECONDLIFE, ipoque_struct, IPQ_LOG_DEBUG,
"Second Life detected.\n");

ipoque_int_secondlife_add_connection(ipoque_struct);

return;
```

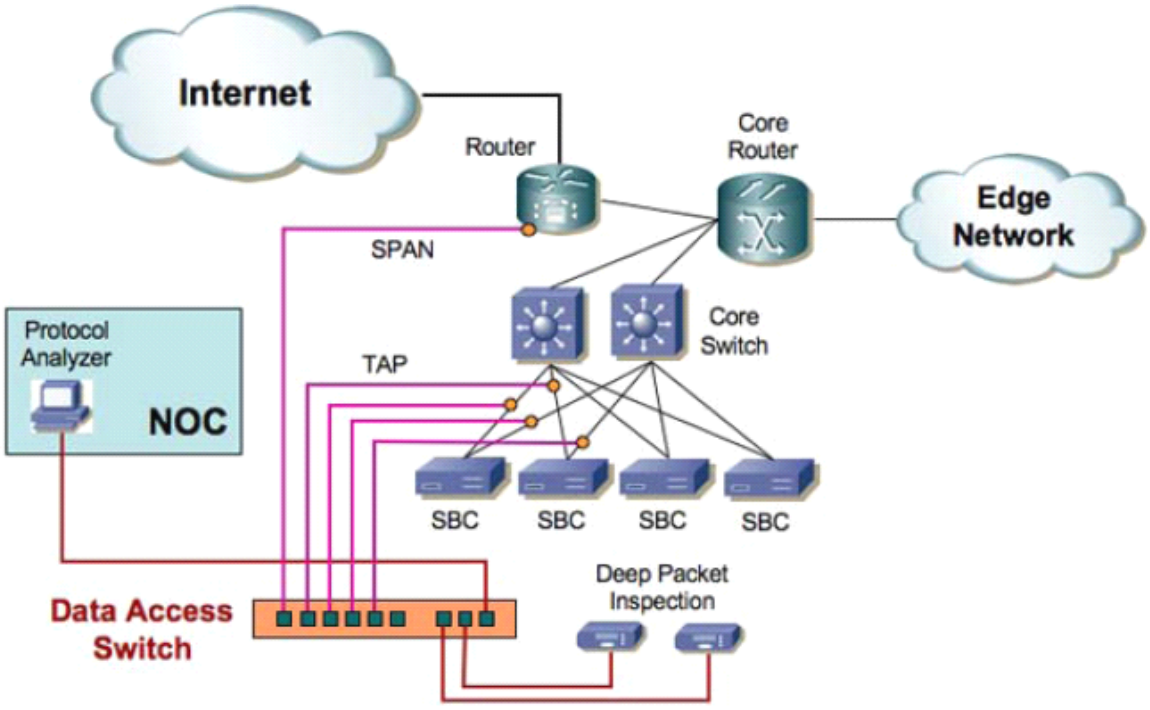
Kaynak koduna aşağıdaki adresden bakılabilir:

http://code.google.com/p/opendpi/source/browse/#svn/trunk/src/examples/OpenDPI_demo

DPI ALTYAPıSı İÇIN GEREKENLER

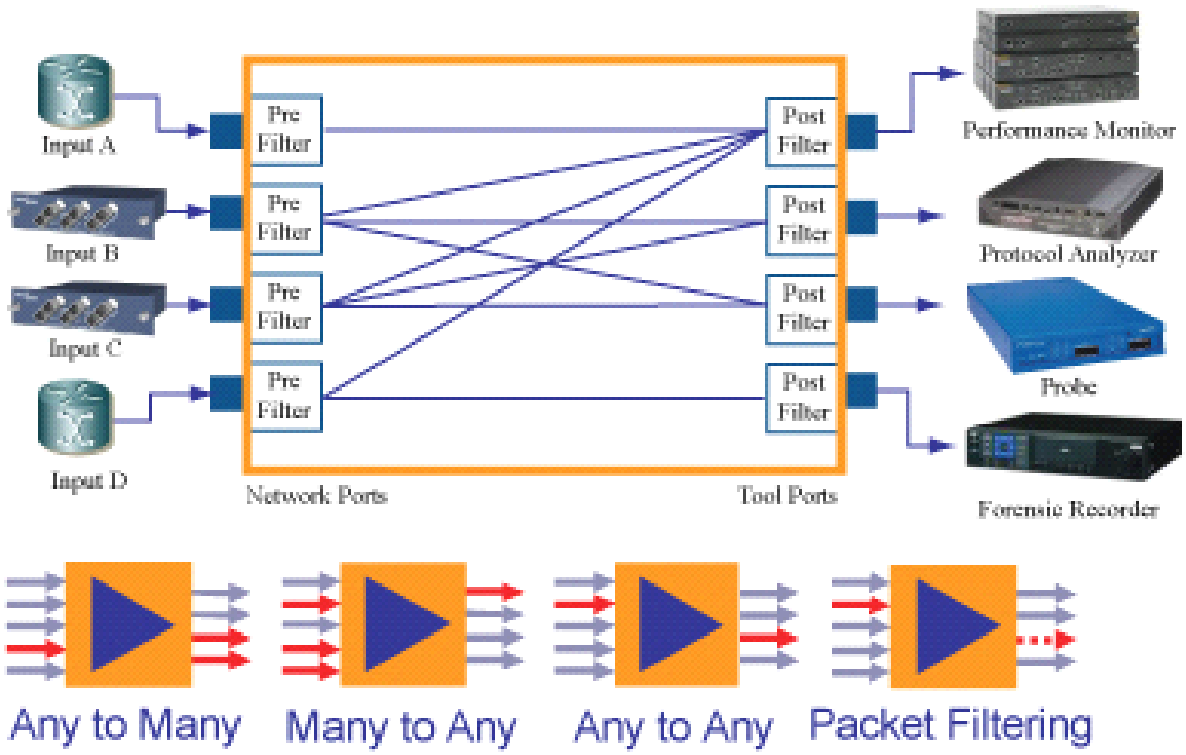
Ağ trafiğinin Derin Paket İnceleme uygulamalarıyla incelenebilmesi için donanım ve yazılımlardan oluşan bileşenlerle uygun bir altyapısının kurulması gerekmektedir.

DPI ürünleri paketlerin filtrelenmesi, analizi, kaydedilmesi v.b. gibi bileşenleri içerek şekilde tek bir kutu olarakta üreticiler tarafından piyasaya sunulmaktadır.



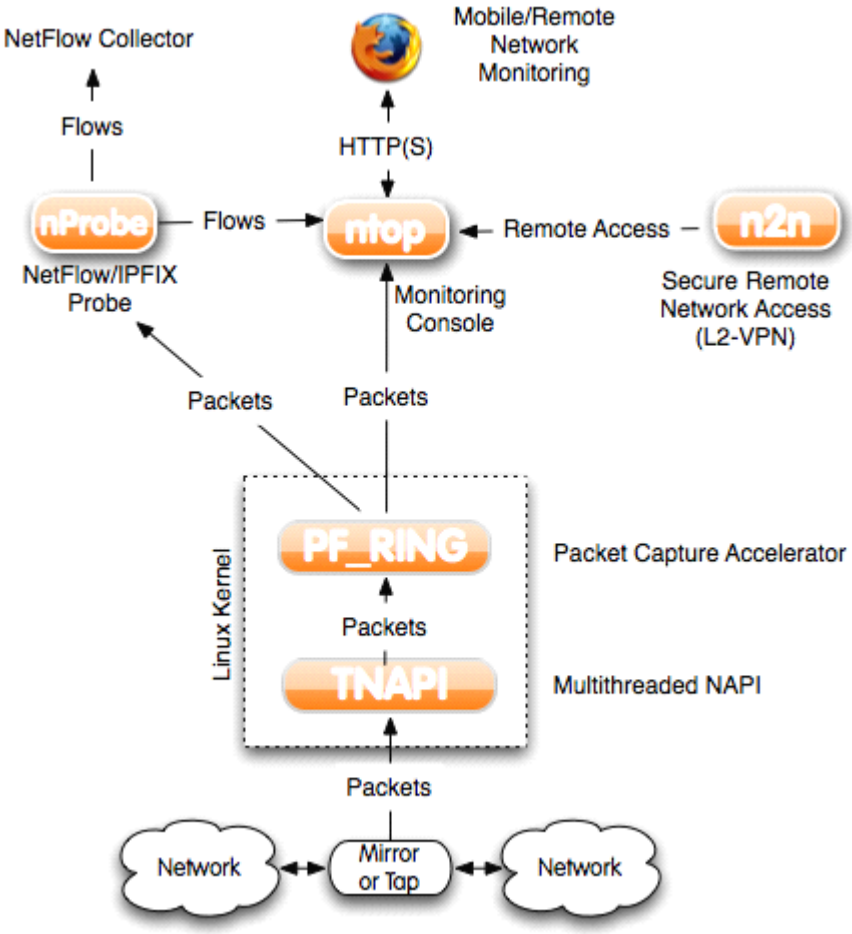
Long-Distance Carrier Core Network

Yukarıdaki şekillerdeki gibi internet trafiğine kanca atılır (tap) daha sonra trafik switchlerde birleştirilebilir ve sonunda da derin paket incelemesi yapılır.



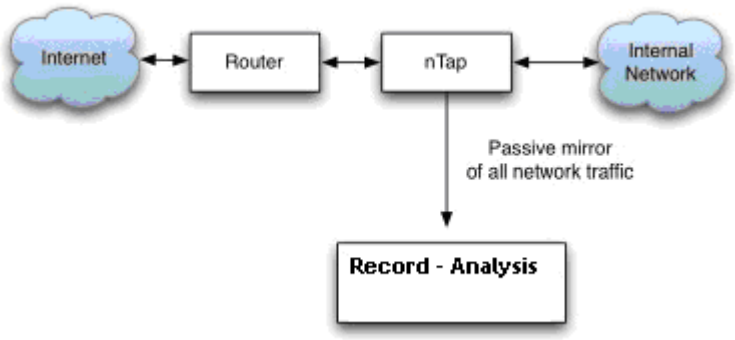
Farklı kaynaklardan gelen trafik yukarıdaki şekilde filtrelenerek yönlendirilir.

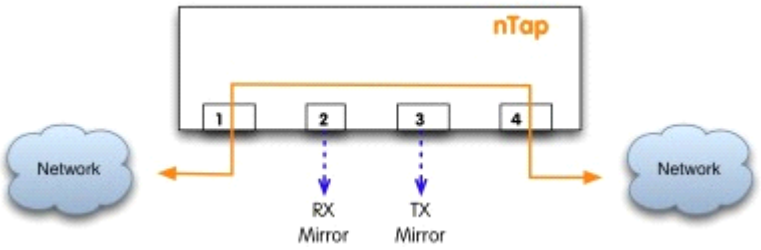
http://www.nmon.net/ DPI çözümlerinde altyapı olarak kullanılacak bileşenleri anlamak için örnek olarak verilebilir:



Kanca Atma – Tapping -Mirror

Ağ trafiği İngilizcede Tap (Test Access Port) adı verilen donanımlar vasıtaylı inceleme amaçlı kopyalanır. Bu sayede akan trafiğe herhangi bir müdahale olmadan inceleme yapılabilir.





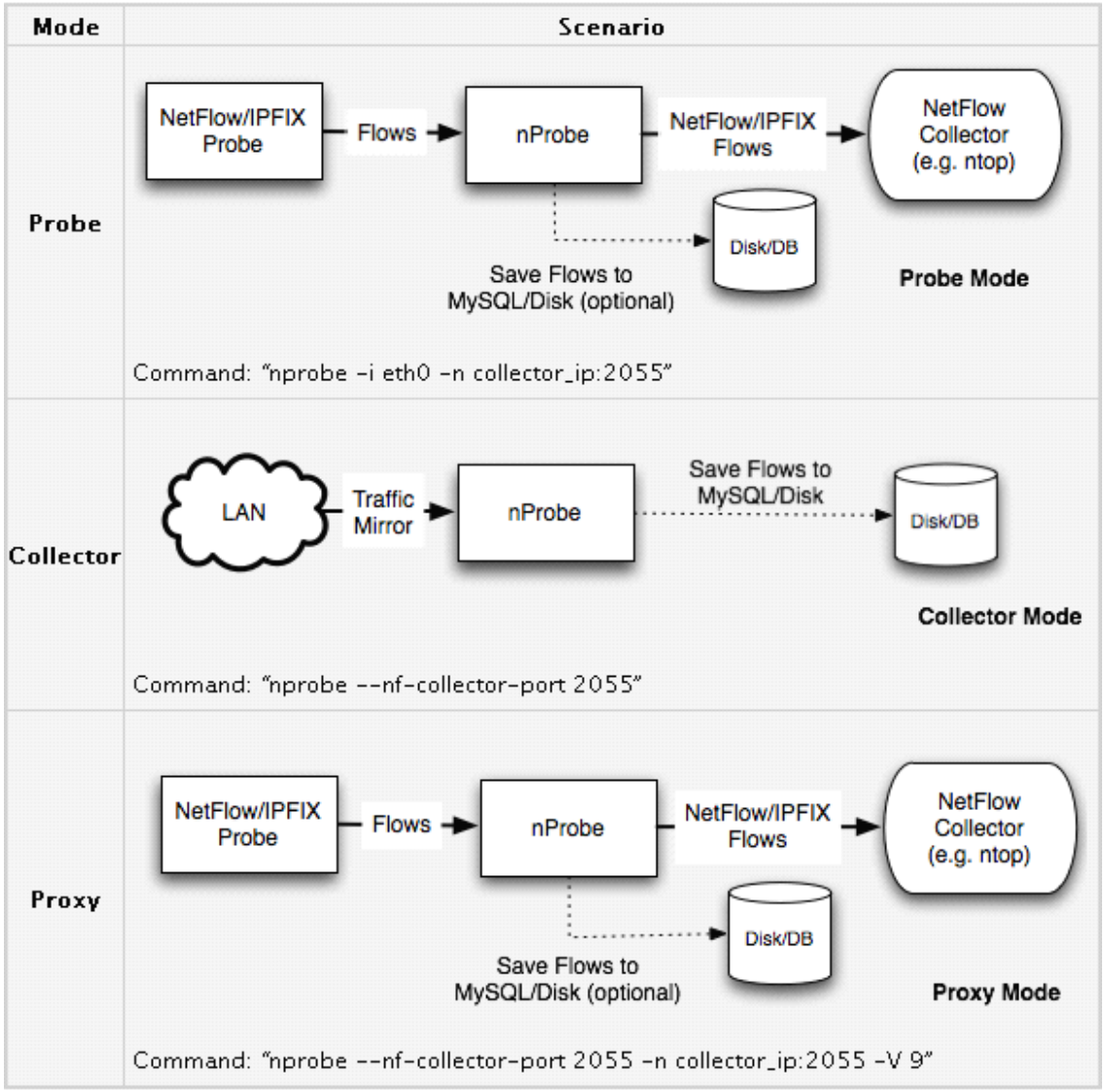
Bu konuda ayrıca mirror denilen donanımlarda aynı işi yapmaktadır.

Paket Yakalama ve Filtreleme

Analiz v.b. amaçla ağ trafik paketleri yakalanır ve filtrelenir.

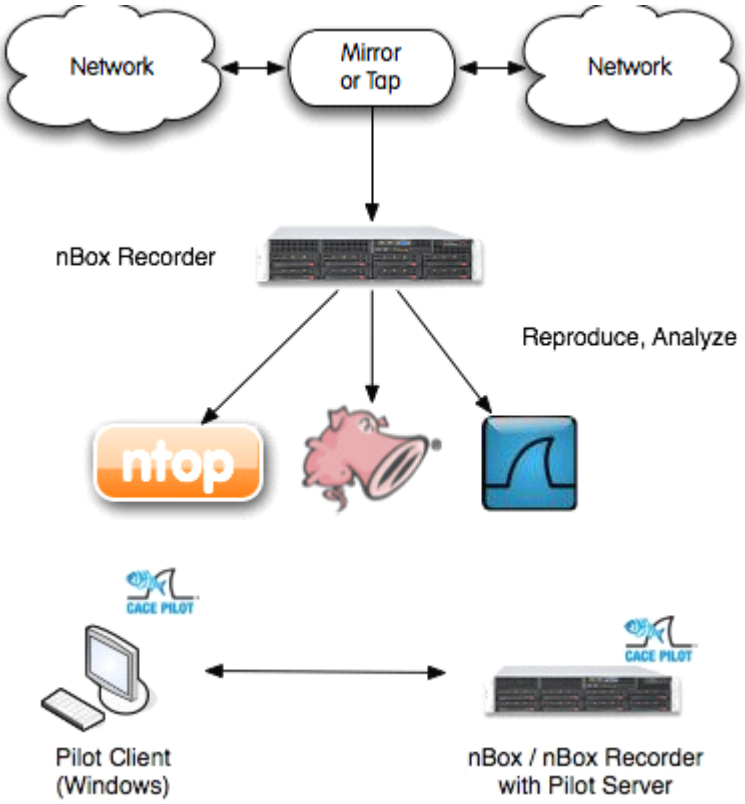
Paket ve Trafik Analizi

Cisco NetFlow v5/v9/IPFIX formatı kullanarak geliştirilmiş çok sayıda yazılım vardır. Bu yazılımlara probe ismi verilir. Probe ağ görüntüleyicisi ve protokol analiz edicisidir. Genelde bir donanıma gömülü olarak kullanılmaktadır. Bu yazılımlar sayesinde trafik akışları toplanır, birleştirilir ve analiz için başka uygulamalara aktarılır. Örneğin nmon organizasyonunun ürünlerinde nBox donanımı NetFlow probe –nProbe- ve trafik birleştirici -ntop- (v5/v9/IPFIX NetFlow flows) içermektedir. ntop network trafiğini popular Unix komutları gibi gösteren açık kaynak kodlu bir yazılımdır. Ntop libpcap üzerine yazılmış ve Unix ve Windows ortamlarında çalışabilmektedir. (ntop-1)



Paketlerin Kayıt Edilmesi

Analiz yapılması için yakalanan paketlerin kayıt edilmesi gerekir. Kayıt sırasındaki en büyük sorun elde edilen hızda kayıt edebilecek disk yani donanım gereksinimidir.



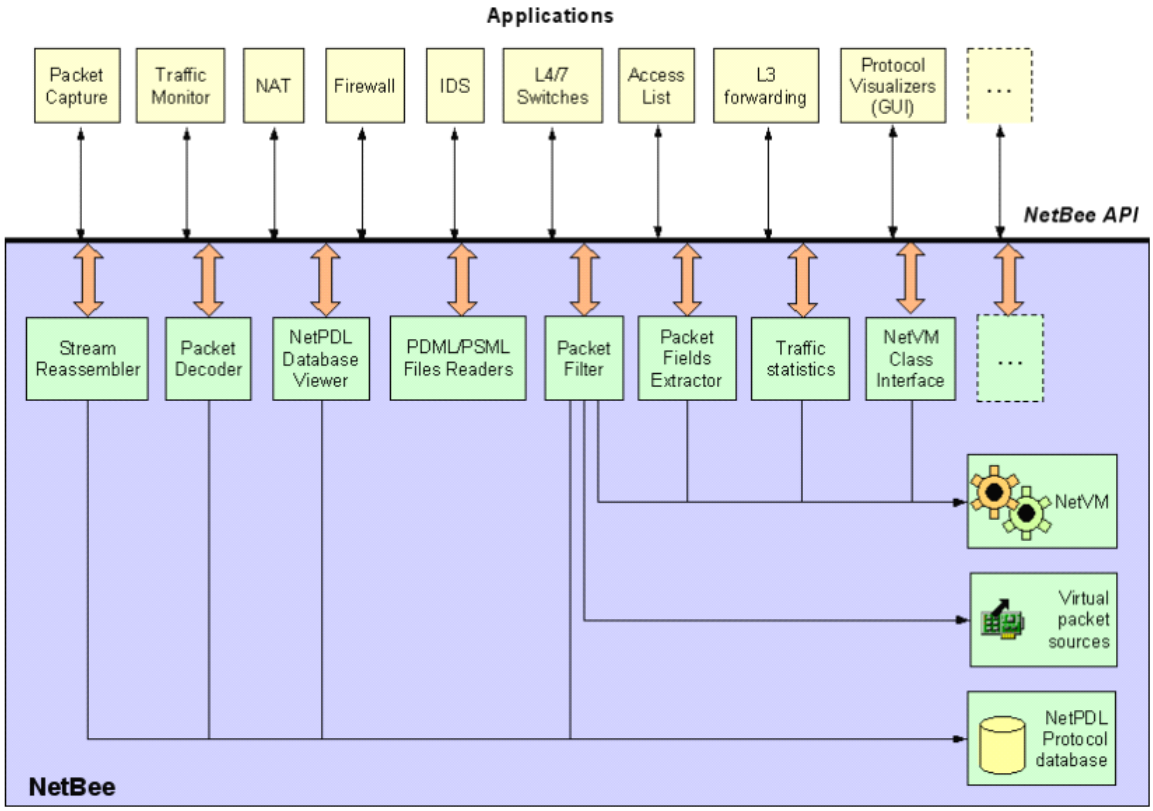
Paket İşleme

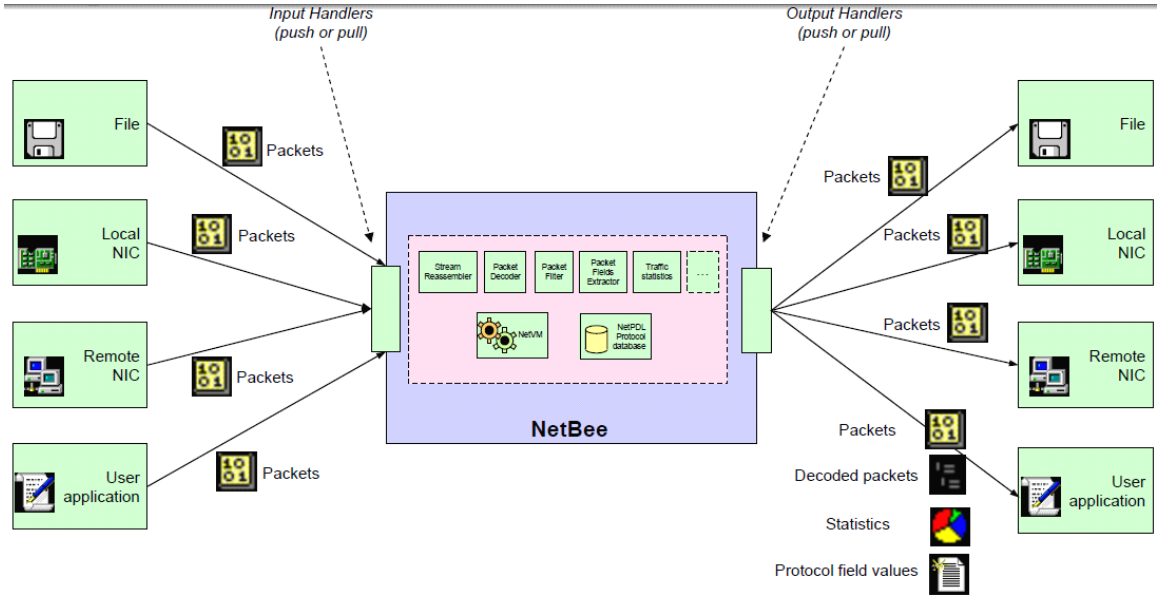
NetBee

NetBee çeşitli paket işleme özelliklerine sahip bir yazılım kütüphanesidir. Binary olarak indirilip kullanılabilmektedir. (netbee-1)

NetBee aşağıdaki konularda kullanılabilir:

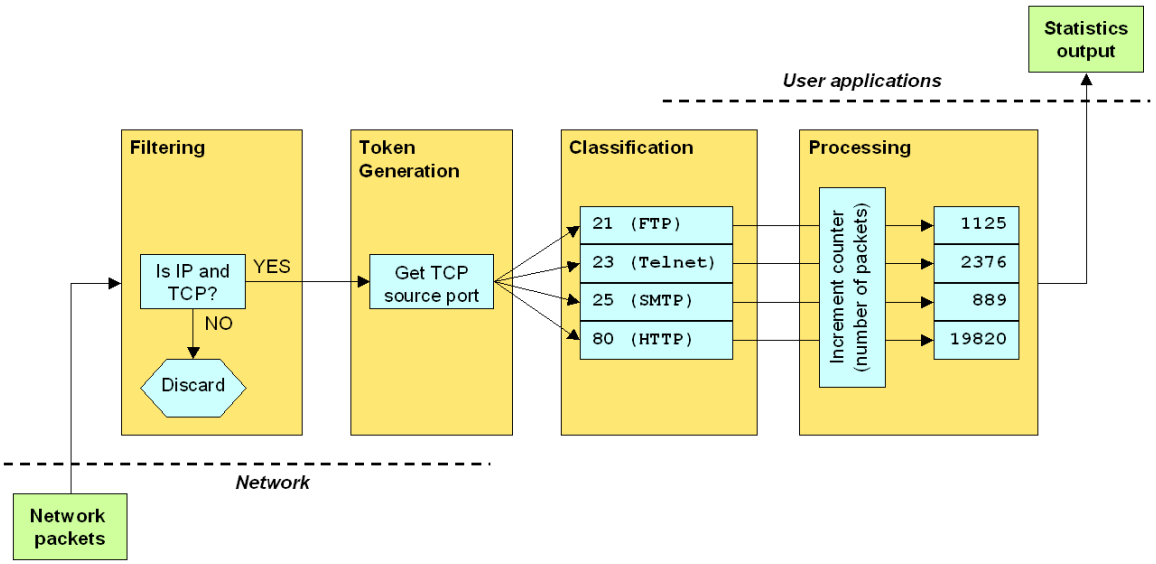
- paket koklama ve filtreleme - packet sniffing and filtering
- paket çözme - packet decoding
- trafik sınıflandırma - traffic classification (henüz) hazır değil

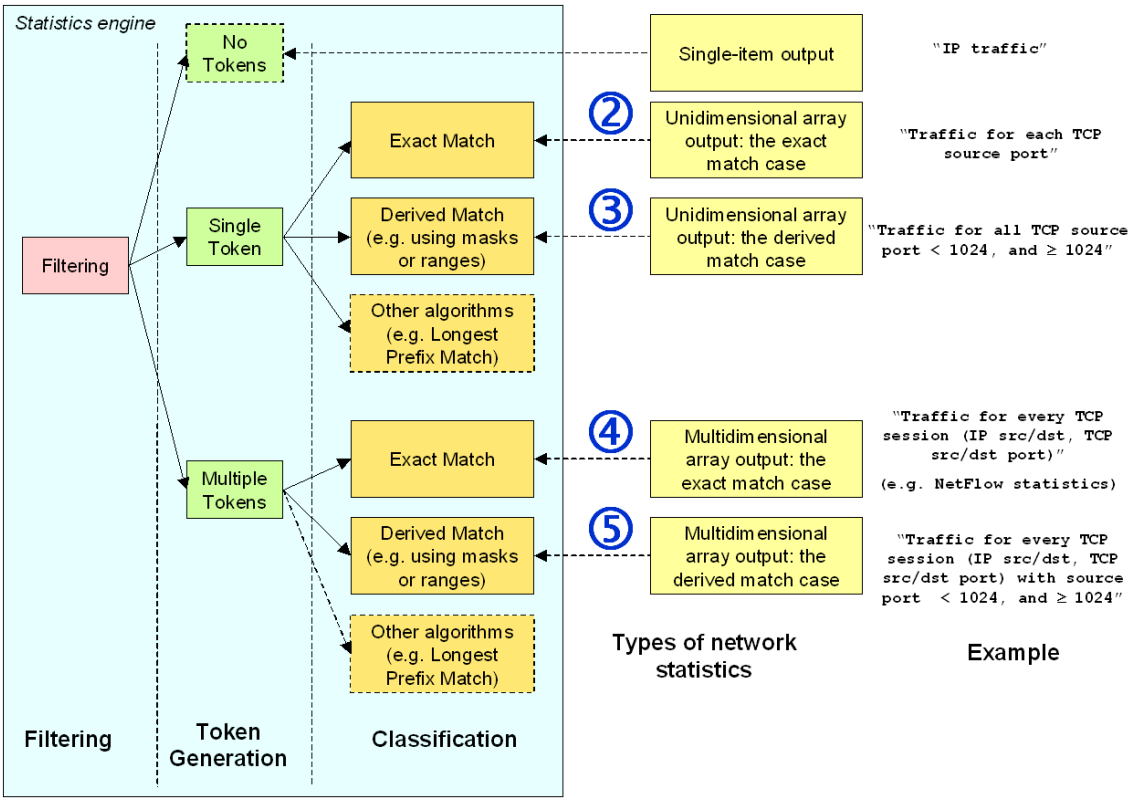

Applications
Packet Capture
Traffic Monitor
NAT
Firewall
IDS
L4/7 Switches
Access List
L3 forwarding
Protocol Visualizers (GUI)
...
NetBee API
Stream Reassembler
Packet Decoder
NetPDL Database Viewer
PDML/PSML Files Readers
Packet Filter
Packet Fields Extractor
Traffic statistics
NetVM Class Interface
...
NetVM
Virtual packet sources
NetPDL Protocol database
NetBee

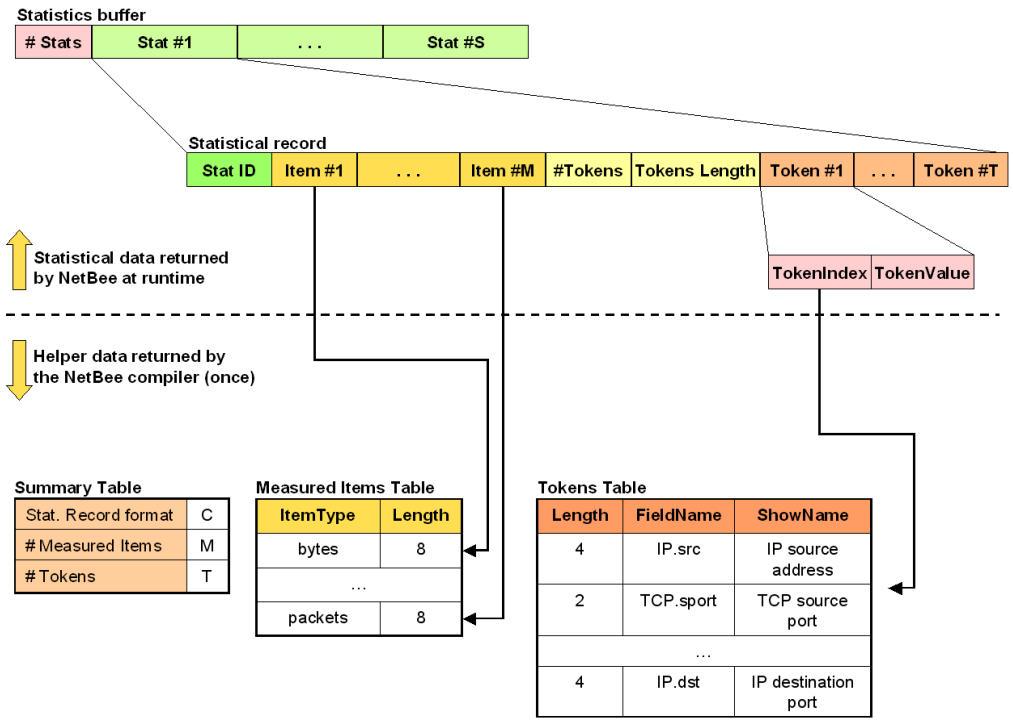

Input Handlers (push or pull)
Output Handlers (push or pull)
File
Local NIC
Remote NIC
User application
Packets
Stream Reassembler
Packet Decoder
Packet Filter
Packet Fields Extractor
Traffic statistics
NetVM
NetPDL Protocol database
NetBee
Decoded packets
Statistics
Protocol field values

NetBee Network Trafik İstatistikleri

NetBee in paketler analiz edildikten sonra network trafiklerine yönelik system mimarisi aşağıdaki şekildedir. (netbee-2)







KAYNAKLAR

Huawei-1: http://www.huawei.com/products/datacomm/catalog.do?id=1235

Esoft-1: http://www.net-spec.com/whitepapers/MigrationtoDPI.pdf

Forrester-1: http://www.csoonline.com/article/494208/Forrester_Deep_Packet_Inspection_As_An_Enabling_Technology?page=2

nProbe-1:http://www.ntop.org/nProbe.html

ntop-1:http://www.ntop.org/overview.html

nmon-1:http://www.nmon.net/recorder.html

Y.dpireq -1: https://datatracker.ietf.org/documents/LIAISON/file617.pdf

dpacket-1: https://www.dpacket.org/articles/deep-packet-inspection-2009-market-forecast

netbee-1: http://www.nbee.org/doku.php?id=docs:overview

netbee-2: http://www.nbee.org/misc/statistics/