Flow Analysis Versus Packet Analysis. What Should You Choose?

www.netfort.com

Flow analysis can help to determine traffic statistics overall, but it falls short when you need to analyse a specific conversation in depth. Packet capture gives you ‘names’ = websites, users, applications, files, hosts, and so on. You can identify individuals and their access to and usage of resources.

Network traffic analysis is a technique used to look at communication patterns on a computer network. “Traffic analysis is the process of capturing and examining network data in order to deduce information from patterns in communication” [1]. In general, the more data that you capture, the more you can infer from the traffic. There are two main technologies that you can choose from if you want to perform traffic analysis on your network; **flow analysis** and **packet analysis.**

What is flow analysis?

A flow is a traffic stream with a common set of identifiers. Typically, a flow is defined by traffic that has the same source IP, destination IP, protocol, source port, and destination port. If any of these variables change, then a new flow is defined. For example, when a client is connecting to a server, several flows might be created because the client might establish several connections to the server, involving new source ports. Each one of these connections would be a separate flow. NetFlow, sFlow, IPFIX are all ways to collect information about traffic that is traversing a network.

NetFlow exports data flow information in UDP datagrams in one of following formats

Version	Description
v1	Similar to v5 but without sequence numbers or BGP info
v2	Never released
v3	Never released
v4	Never released
v5	Fixed format, most common version found in production
v6	Never released
v7	Similar to v5 but without TCP flags, specific to Cisco Catalyst 500 and 6000
v8	Aggregated formats, never gained wide use in the enterprise
v9	Next generation flow format found in most modern NetFlow exporters, supports IPv6, MPLS, Multicats and many others
IPFIX	Similar to v9 but standardized and with variable length fields

Devices such as routers or switches along the traffic path can generate flow data, based on the traffic that is traversing them. The flow data is sent to a **flow collector**, which then creates reports and statistics from the flow updates. This process is called **flow analysis**. The packets sent to a flow collector are not copies of the actual packets in the traffic flow, as is the case in a SPAN port. The flow analysis packets carry statistical data regarding the flow. Flow-based reporting is a good way to understand what traffic is traversing the network. Most NetFlow collection applications deployed today use NetFlow version 5, which tracks the following key fields:

- Source interface
- Source and destination IP address
- Layer 4 protocol (for example, ICMP, TCP, UDP, OSPF, ESP, and so on)
- Source and destination port number (if the layer 4 protocol is TCP or UDP)
- Type of service value

NetFlow v9 and Internet Protocol Flow Information Export (IPFIX) are available on some Cisco Integrated Services Routers (ISRs) and Cisco ASR 1000 Series Aggregation Services Routers (ASR1ks) with Next Generation Network based Application Recognition (NBAR2) enabled. These device features will allow you to capture application information but has very limited support in most NetFlow collectors.

What is packet analysis?

Although flow-based analysis solutions are great, there are some areas where packet capture and analysis is still needed. Packet analysis is normally associated with **SPAN** or **mirror ports**, which are available on most managed network switches. "**Port mirroring** is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port" [2]. Port mirroring on a Cisco Systems switch is generally referred to as **Switched Port Analyser** (SPAN); some other vendors have other names for it, such as Roving Analysis Port (RAP) on 3Com switches.

Deep packet inspection (**DPI**) applies to technologies that use packets as a data source and then extract metadata such as application or website names. In contrast, flow data in most cases does not provide any information about what is contained within packet payloads.

For this reason, when analysing an application, it is critical to use packet capture solutions because they let you see the actual packets involved in client conversations and identify the root cause of an issue. Content-based application recognition, which is based on Deep Packet Inspection, can identify traffic by application, even when unusual or dynamic port numbers are used.

NETFORT
know your network

Flow Analysis versus Packet Analysis – For Internet Monitoring

	Flow Analysis Tools	Packet Capture
Vendor agnostic	No	Yes
Username association	No	Yes
Accurate web domain reports	No	Yes
Resource (URI) names	No	Yes
Proxy reporting	No	Yes
Bandwidth usage	Yes	Yes
HTTP header analysis	No	Yes
Port 80 analysis	No	Yes
SMTP monitoring	No	Yes
BitTorrent decoding	No	Yes
DNS SPAM detection	No	Yes
Web client detection	No	Yes
Security/IDS	No	Yes
Passive hostname capture	No	Yes
Resource sizes (files)	No	Yes
Real-time data	Yes	Yes
Historical data	Yes	Yes

Flow Analysis versus Packet Analysis – For User & Application Monitoring

	Flow Analysis Tools	Packet Capture
Vendor agnostic	No	Yes
Deploy at any point in the network	No	Yes
Accurate application recognition	No	Yes
Username association	No	Yes
Drilldown from application to port number	No	Yes
Drilldown from application to user	No	Yes
True application names	No	Yes
Accurate web domain reports	No	Yes
Resource (URI) names	No	Yes
Proxy reporting	No	Yes
Bandwidth usage	Yes	Yes
HTTP header analysis	No	Yes
Port 80 analysis	No	Yes

SMTP monitoring	No	Yes
BitTorrent decoding	No	Yes
File activity monitoring	No	Yes
Passive hostname capture	No	Yes
Resource sizes (files)	No	Yes
Real-time data	Yes	Yes
Historical data	Yes	Yes
Filter bandwidth usage by MAC address	No	Yes
Filter bandwidth usage by IP address	Yes	Yes
IP flow count reporting	Yes	Yes

Flow Analysis versus Packet Analysis – For Network Security Monitoring

	Flow Analysis Tools	Packet Capture
Vendor agnostic	No	Yes
Username association	No	Yes
Security/IDS	No	Yes
True application names	No	Yes
Resource (URI) names	No	Yes
HTTP header analysis	No	Yes
Web client detection	No	Yes
Port 80 analysis	No	Yes
SMTP monitoring	No	Yes
BitTorrent decoding	No	Yes
DNS SPAM detection	No	Yes
File activity monitoring	No	Yes
Passive hostname capture	No	Yes
Real-time data	Yes	Yes
Historical data	Yes	Yes
Ingress and egress IP flows reports	Yes	Yes
Packets count reporting	No	Yes
IP flow count reporting	Yes	Yes
Detect application layer attacks	No	Yes

Conclusion

Flow analysis can help to determine traffic statistics overall, but it falls short when you need to analyse a specific conversation in depth. A good example of this is web usage tracking. “NetFlow v5 isn't a good tracker because nowhere in the list of fields above do we see HTTP header" [3]. The HTTP header is the part of the application layer payload that actually specifies the website and URL that is being requested.

Which analysis method should we use in a monitoring solution?

Both! When looking at traffic statistics, flow analysis is sufficient if you only want to see IP addresses and how much data they are transferring. However, when you want to troubleshoot performance problems, in many cases you need to see the full packet detail.

What are the main differences between flow capture and packet capture?

1. Flow capture features are normally found on layer 3 type devices like routers. Packet capture uses SPAN or mirror ports which are available on most managed switches.
2. Flow capture gives top-level information like IP addresses and traffic volumes. Packet capture also gives you this and more.
3. Flow capture tools can struggle with the activity associated with content delivery networks and applications that use multiple TCP or UDP ports. If you want accuracy, then packet capture is the way to go.
4. Flow capture does not look at payloads contained within packets unless you are using advanced features like Next Generation Network based Application Recognition (NBAR2).
5. Packet capture gives you ‘names’ = websites, users, applications, files, hosts, and so on. You can identify individuals and their access to and usage of resources.

Try Packet Capture

NetFort LANGuardian is one of the best **Deep Packet Inspection** solutions on the market. To find out more, or for your free trial, contact:

Web: www.netfort.com

E-mail: sales@netfort.com

References

1. http://en.wikipedia.org/wiki/Traffic_analysis
2. http://en.wikipedia.org/wiki/Port_mirroring
3. http://unroutable.blogspot.com/2012/04/why-netflow-isnt-web-usage-tracker.html