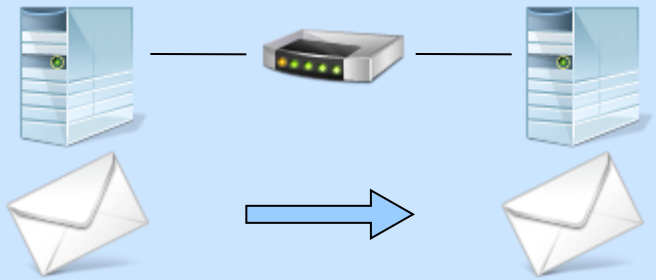
Introduction to Flow Analysis

Vincent Berk

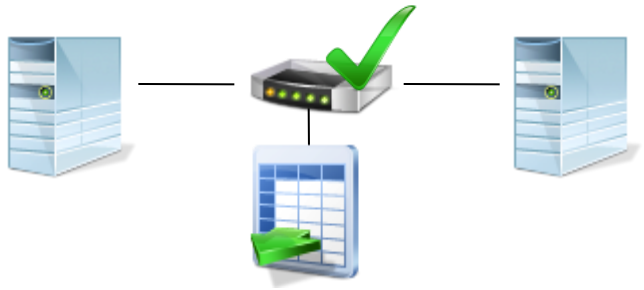
February 3rd , 2011

Overview



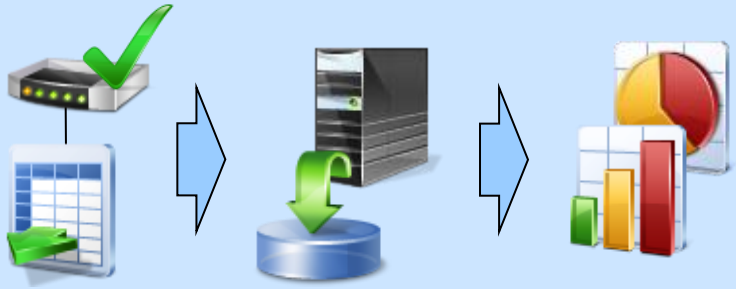
Computers communicate over the network, in streams of thousands of packets.

Actions, such as sending email, result in streams of related packets, called *"flows"*.



Most routers, firewalls, and switches can report summaries of all their flows.

This process of reporting on flows is called *"exporting"* of flows.



Flows are exported to a *"collector"*, which may aggregate, plot, or store the flows.

A collector is a separate program running on a network server.

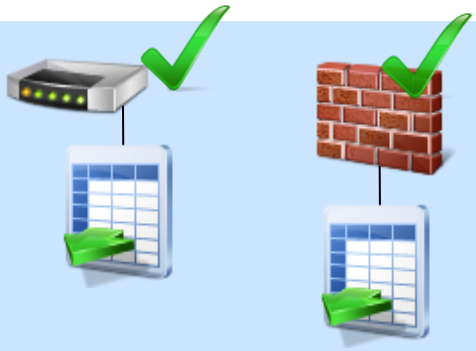
VINCENT BERK

ProQueSys

Exporter

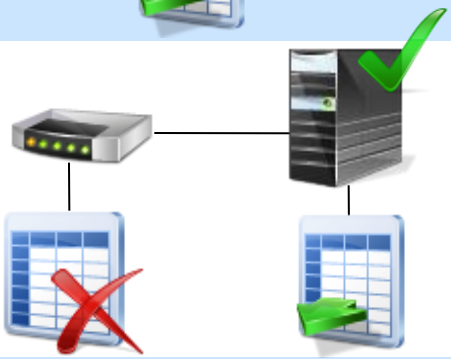
Exporters are routers, firewalls, or switches capable of forwarding flow summaries.

Most top- and middle-tier networking hardware is capable of exporting flow summaries.



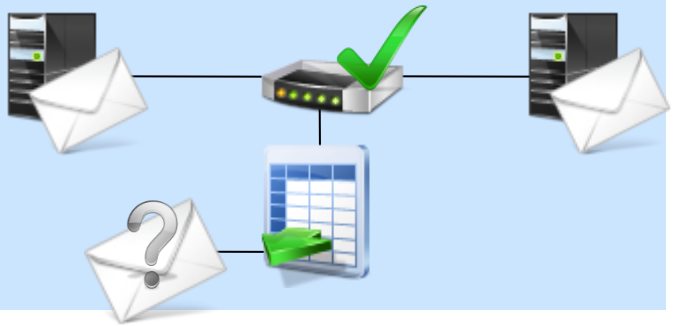
If your hardware is not capable of exporting flows, a software exporter can be used.

This is a program that runs on a computer which must be attached to a SPAN/TAP/Mirror port on a switch or router, and does the flow exporting.



Exported flows are only traffic summaries, they do not contain any traffic content.

For instance: a flow reports the connections to an email server, but not the content of the emails.



ProQueSys

Collector

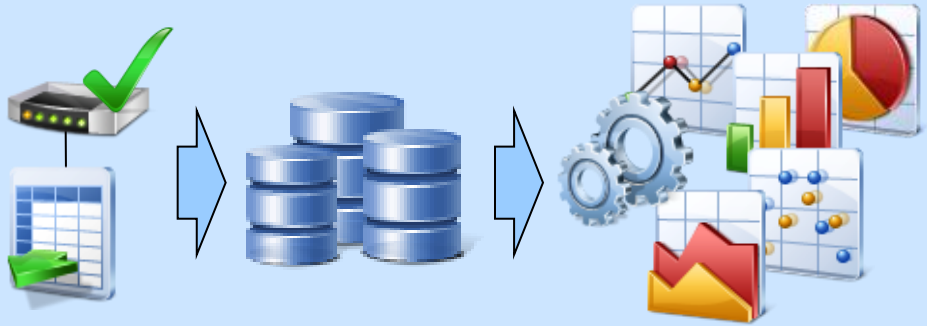
A collector is a server with software that can accept and interpret flow exports.

Exporters send their flow summaries to collectors for storage and analysis.

Most collectors summarize and aggregate the flows before storage, *discarding* the records.

Although coarse, this approach is fastest.

The cost is the loss of forensic accuracy.



Some collectors store *all* flow records, alowing full recall, and precise filtering.

The value of a flow product depends mostly on the implementation of the collector.

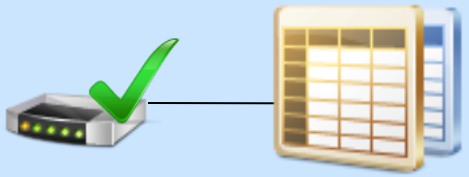
VINCENT BERK

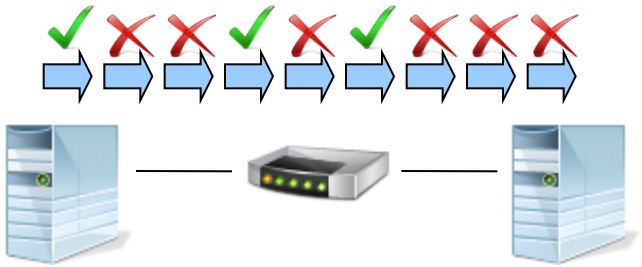
ProQueSys

Flow Formats

Flow exports come in many formats. Some Manufacturers are compatible, others not.

Adding flow capability to your network will increase the traffic load by 1% to 5%.



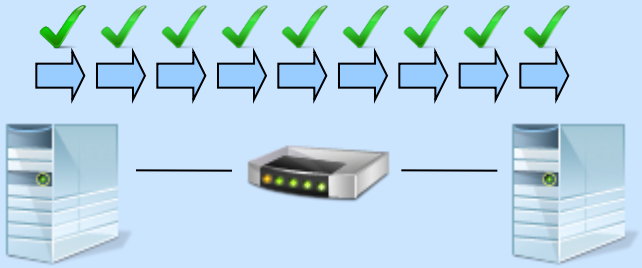


Some flow formats are sampled. This means that only *some* flows are reported on.

Forensic accuracy is lost to gain some speed. *sFlow* ® uses this strategy.

Most flow formats report every flow, allowing full flow recall, if the collector supports this. *NetFlow, Cflow,* and *Jflow* use this strategy.

If your hardware only supports flow sampling, you can always use a software exporter instead.



VINCENT BERK

ProQueSys

For Additional Information:

http://www.proquesys.com

info@proquesys.com

603.727.4477

ProQueSys FlowTraq	A full fidelity flow collector. Supports: IPv6, NetFlow v1/5/7/9, sFlow v2/4/5, automated alerting, scheduled reporting, user dashboards, GUI and CLI interfaces.
ProQueSys Flow Exporter	*FREE* downloadable software flow exporter. Supports: IPv6, exporting in NetFlow v5 and v9, VLAN, IFindex specification, exporters to 16 destinations at once.

PROQUESYS