

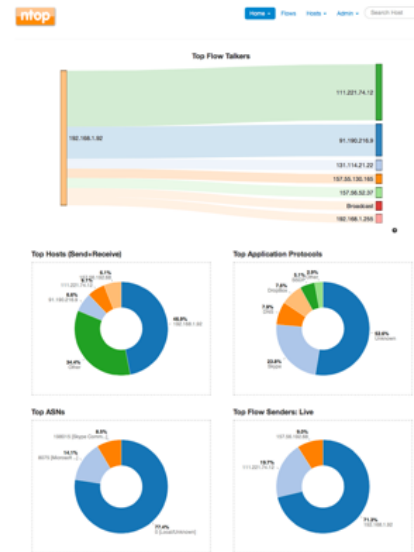
ntop Users Group Meeting

ntop
Visibility, Security Awareness



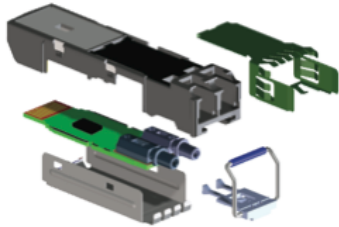
About ntop

- Private company devoted to development of Open Source network traffic monitoring applications.
- ntop (circa 1998) is the first app we released and it is a web-based network monitoring application.



Some Products we Developed [1/2]

- Our software is powering many commercial products...



Integrated ASIC with JDSU technology



Some Products we Developed [2/2]

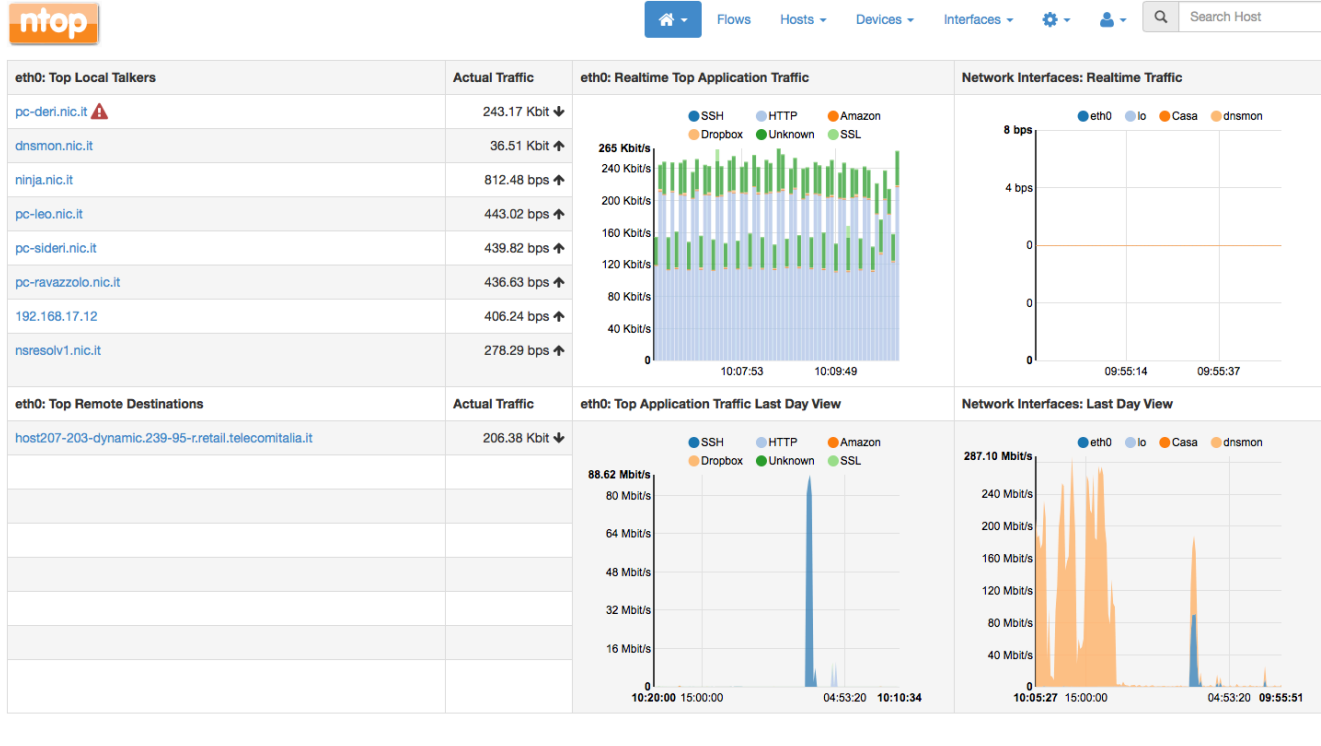
- ...and allows packets to be received and transmitted at 1/10 Gbit line rate with no loss, any packet size on Intel-based commodity NICs.
- So we accelerate not just our applications but also third party open source solutions including:



Product Lines

- Open Source
 - ntopng: Web-based monitoring application
 - PF_RING: Accelerated RX/TX on Linux
 - nDPI: Deep Packet Inspection Toolkit
- Proprietary
 - PF_RING ZC: 1/10/40/100 Gbit Line rate.
 - nProbe: 10G NetFlow/IPFIX Probe
 - nProbe Cento: flows+packets+security
 - n2disk/disk2n Network-to-disk and disk-to-network.
 - nScrub: Software DDoS Mitigation

ntopng: Web-based Monitoring



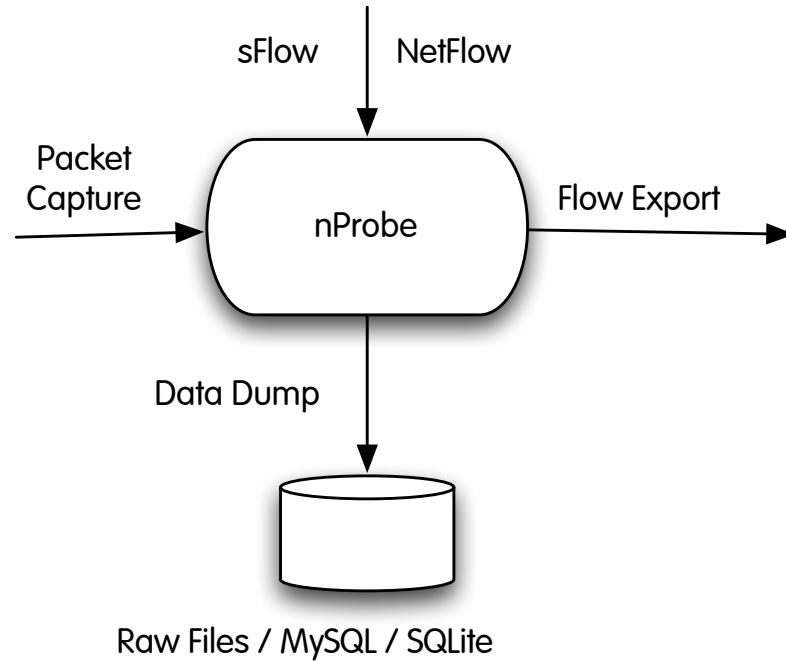
ntopng Enterprise v.2.5.161002
User **admin** Interface **eth0**

284.05 Kbps [76 pps] 206.34 Kbps 30.58 Kbps

Uptime: 16 h, 6 min, 45 sec
▲ 10,694 Alerts 71 Hosts 1,248 Devices 107 Flows



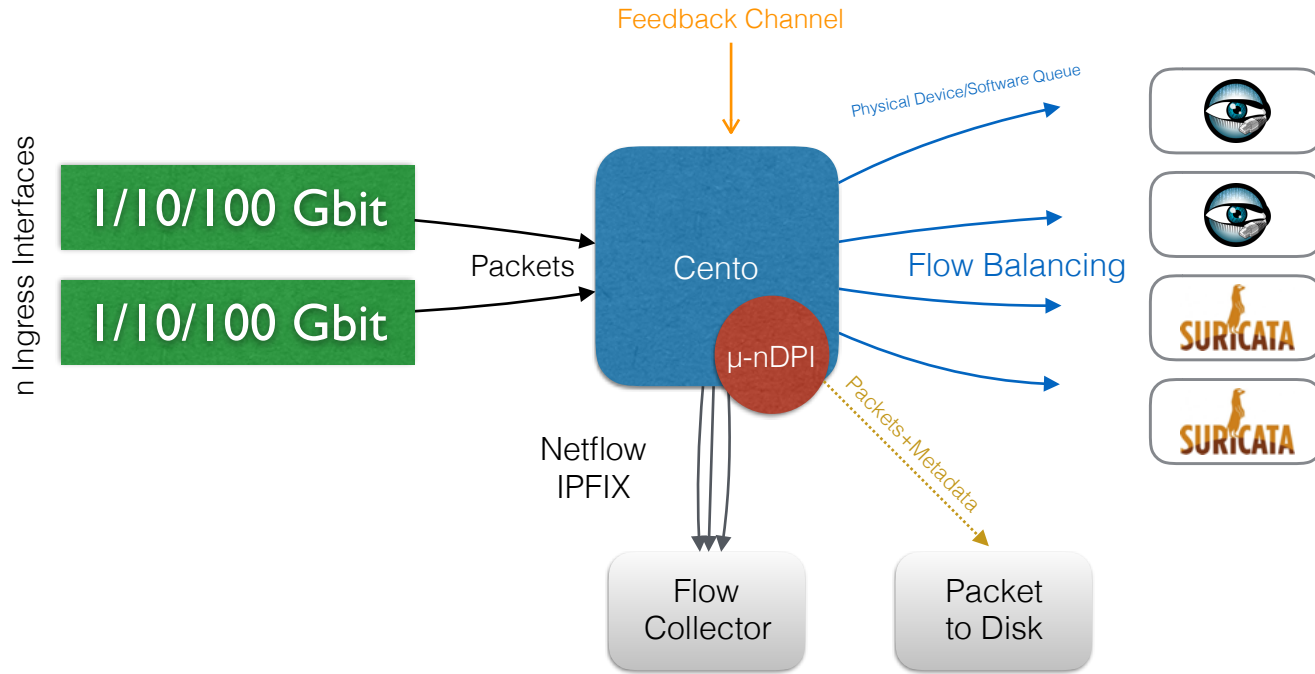
nProbe: Flow-based Traffic Probe [1/2]



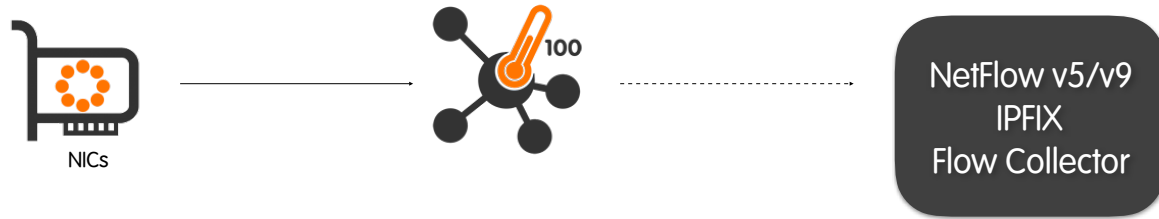
nProbe: Flow-based Traffic Probe [2/2]

- Extensible, NetFlow/IPFIX-based probe and collector.
- Available for Unix (Linux, *BSD, OSX...) and Windows.
- Small memory footprint that make it suitable to be embedded on small appliances (appneta.com), used on the cloud (kentik.com), or deployed on an nBox.
- Big-data aware (Kafka, Elastic Search).
- Plugins for dissecting popular Internet (HTTP, Email, VoIP...), ISPs (Radius, Diameter..), Mobile (GTPv 0/1/2, S1AP) and application protocols (MySQL, FTP...)

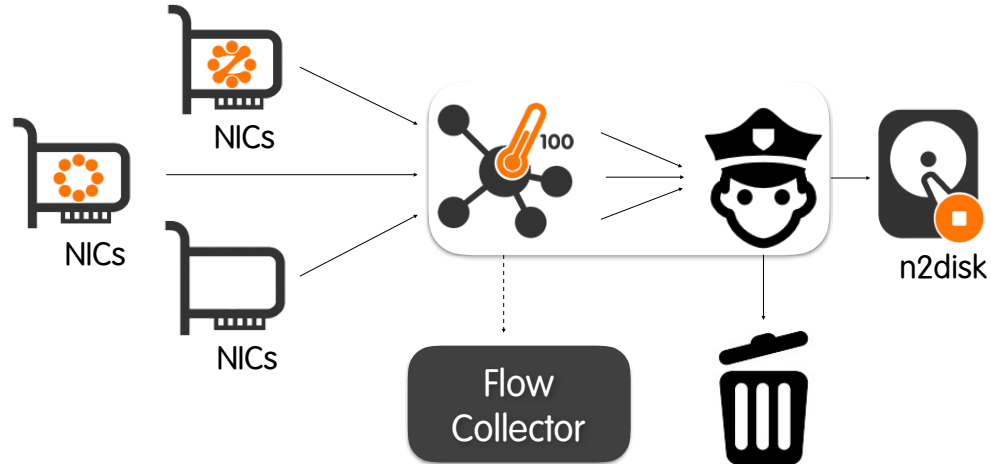
nProbe Cento



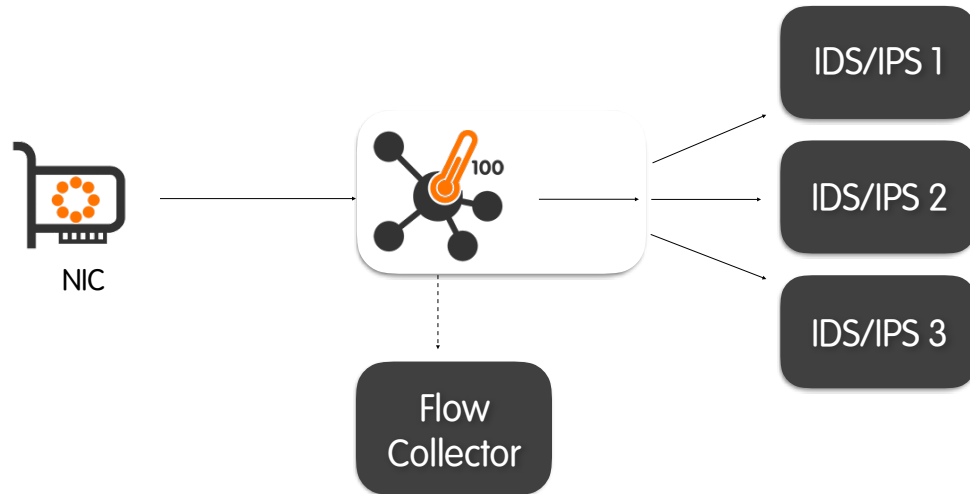
Centos: Flow Generation

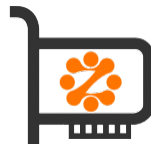


Centos: Packet to Disk



Centos: IDS/IPS





- PF_RING is a home-grown open source packet processing framework for Linux.
- Support of legacy pcap-based applications as well FPGA NICs.

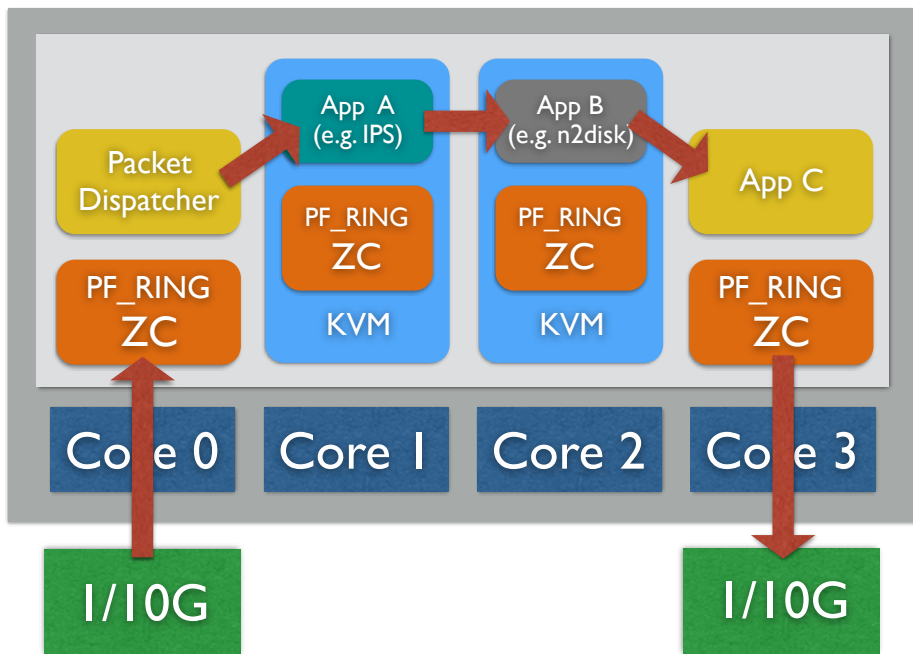


- ZC has simple yet powerful components (no complex patterns, queue/consumer/balancer).
- KVM/Docker/OpenStack support: ability to setup Inter-VM clustering.
- Native PF_RING ZC support in many open-source applications such as Snort, Suricata, Bro, Wireshark.



PF_RING ZC [2/2]

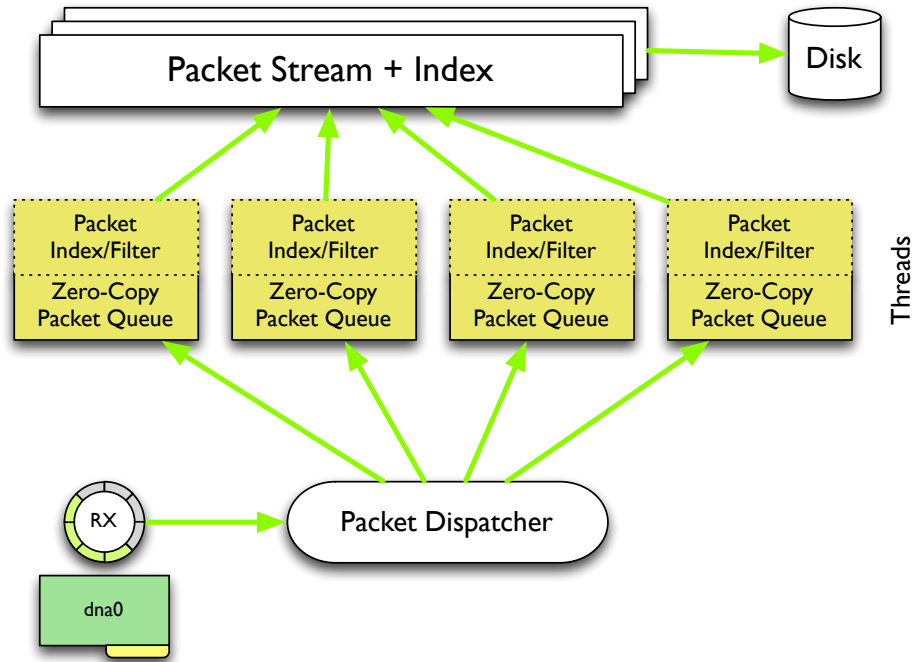
```
(Host) $ ./zpipeline_ipc -i zc:eth2,0 -o zc:eth3,1 -n 2 -c 99 -r 1 -t 2 -Q /tmp/qmp0  
(VM) $ ./zbounce_ipc -c 99 -i 0 -o 1 -g 3
```



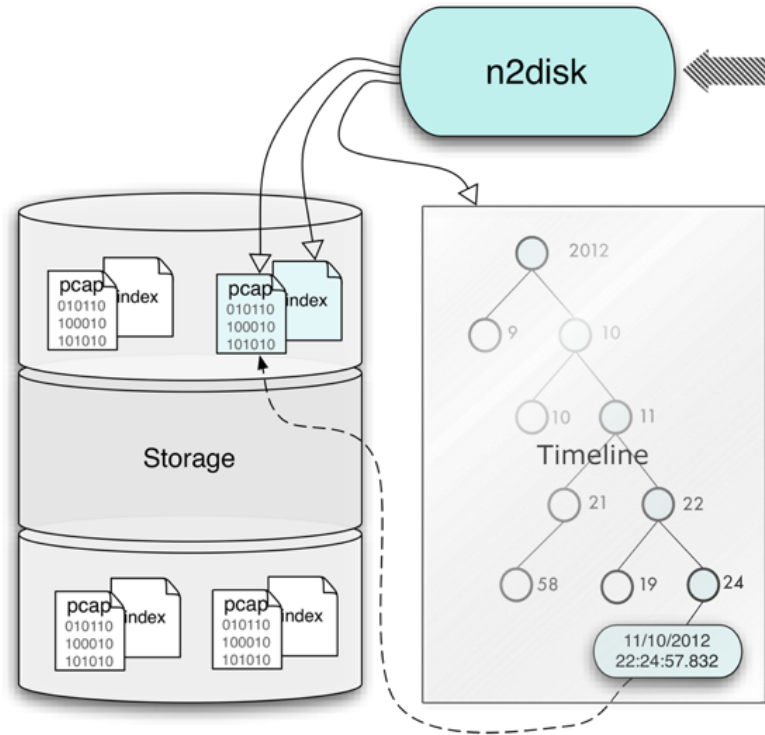
- ntop has decided to develop its own GPL DPI toolkit in order to build an open DPI layer for ntop and third party applications.
- Supported protocols (> 200) include:
 - P2P (Skype, BitTorrent)
 - Messaging (Viber, Whatsapp, MSN, The Facebook)
 - Multimedia (YouTube, Last.fm, iTunes)
 - Conferencing (Webex, CitrixOnline)
 - Streaming (Zattoo, Icecast, Shoutcast, Netflix)
 - Business (VNC, RDP, Citrix, *SQL)



n2disk: Packet to Disk



n2disk Packet Timeline



disk2n: Playing-back Network Traffic

- pcap files written by n2disk can be reproduced using popular tools such as tcpdump or pfsend.
- n2disk comes with a companion tool named disk2n that allows to
 - Reproduce pcap files at the same rate as they were received.
 - Use the same sw timestamping technology used by n2disk to send packets at a high precision rate.
 - Reproduce multiple pcap files (multi-TB) for long-run traffic replay.



nBox

- Intel-based network Appliance for
 - Flow generation 1/10 Gbit
 - Packet-to-disk and disk-to-network



Extract Packets

From: 2013-01-30 23:39:00

To: 2013-01-30

Filter: ip host 192.168 BPF-Like filter for

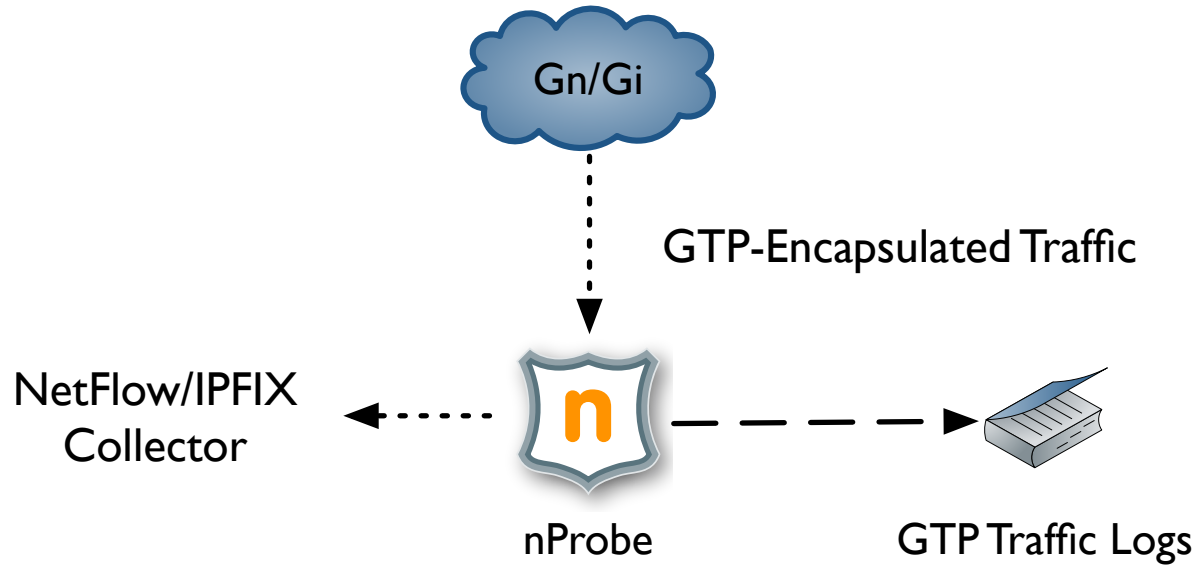
Output File: /storage/n2disk

Specify where the file does not exist, it will be created.

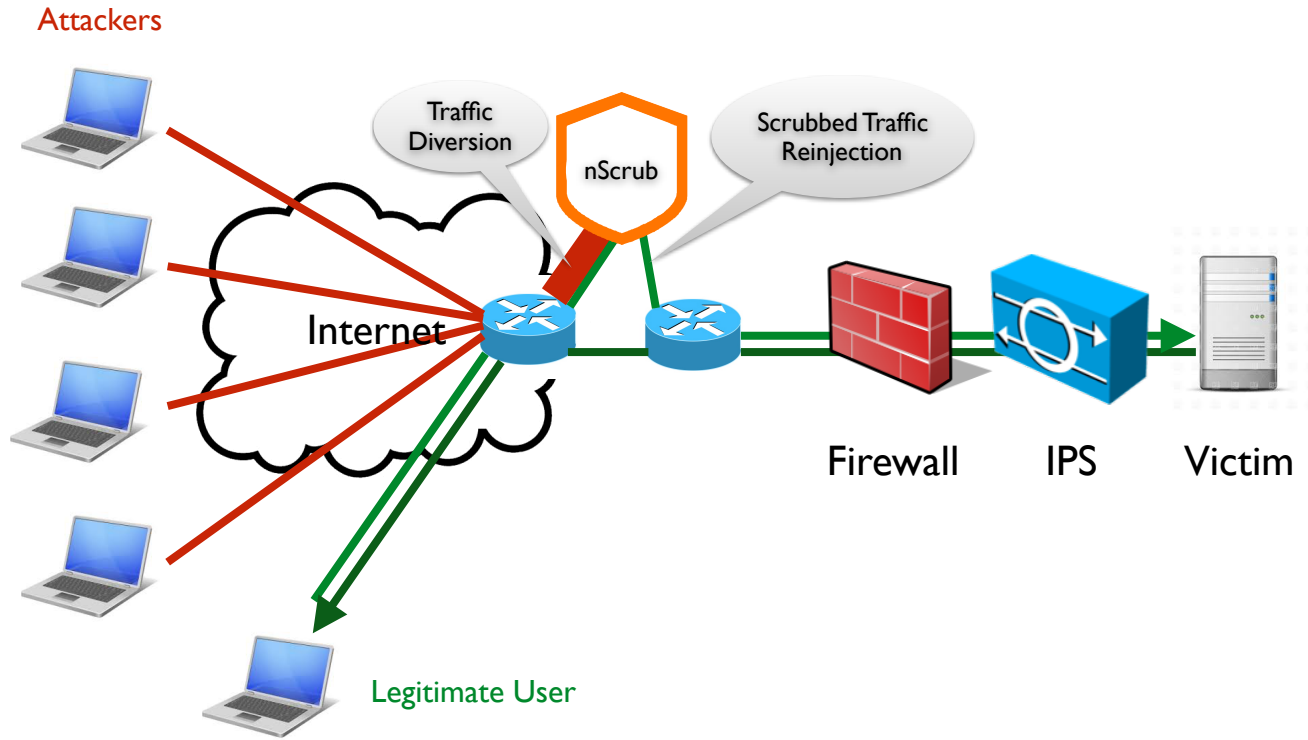
NOTE: you can download the file via FTP or SSH. Please configure a login name and password in the Users Configuration web page.

Start Extraction

nProbe for Mobile Operators



nScrub: 10 Gbit DDoS Mitigation



The Big Picture

- We have developed components that can fulfil various requirements:
 - Traffic visibility (DPI, L7-Protocol support).
 - User-to-IP-to-Category characterisation.
 - Data retention and troubleshooting (n2disk).
 - Graphical console for network monitoring (ntopng).
 - Multi-10 Gbit support (RX+TX), balancing, filtering....
 - DDoS Mitigation
 - 100 Gbit traffic monitoring (QoS + QoE)
- In essence we're working towards a toolkit for commodity hardware systems, able to satisfy most network monitoring needs.