Advanced Logging

```
pip3 install --user scapy-nflog-capture pagerduty-api
```

```
python3 -c 'from pagerduty_api import Alert; from scapy.all import *; from nflog_cffi import NFLOG; import os; os.fork() == 0 and (lambda
nflog: (lambda fd, nf: [Alert(service_key="xxx").trigger(client_url="http://mysite.com", client = "my-client", description = "attempted
access to {}\n".format(IP(pkt).dst)) for pkt, _, _ in nf])(next(nflog), nflog)(NFLOG().generator(3, extra_attrs=["len", "ts"],
nlbufsiz=2*2**20)))'
```

Flowtables

Bypass the network stack (fastpath) / HW offloading

```
ip link add dummy0 type dummy
ip link add dummy1 type dummy

nft add table inet flow_table
nft add chain inet flow_table forward '{ type filter hook forward priority filter; }'

nft add flowtable inet flow_table f_t "{ hook ingress priority 0; devices = { dummy0, dummy1 }; }"

nft add rule inet flow_table forward ip protocol { tcp, udp } flow offload @f_t
nft add rule inet flow_table forward ip6 nexthdr { tcp, udp } flow offload @f_t

nft add rule inet flow_table forward ct state established,related counter return
nft add rule inet flow_table forward ip protocol { tcp, udp } return
nft add rule inet flow_table forward ip6 nexthdr { tcp, udp } return
```

https://www.kernel.org/doc/html/latest/networking/nf_flowtable.html#hardware-offload