NFShunt: OpenFlow Firewall Acceleration

Christopher Lorier
REANNZ

Firewalls

- Achieve high throughput with parallelisation.
- Support thousands of separate flows
- Not as good at supporting a lot of throughput for a single flow
- Not so good for big data

PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE
TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON

Boring Solutions

Buy a bigger Firewall

- Somewhere in the order of $100k for 10Gbps firewall

ACLs

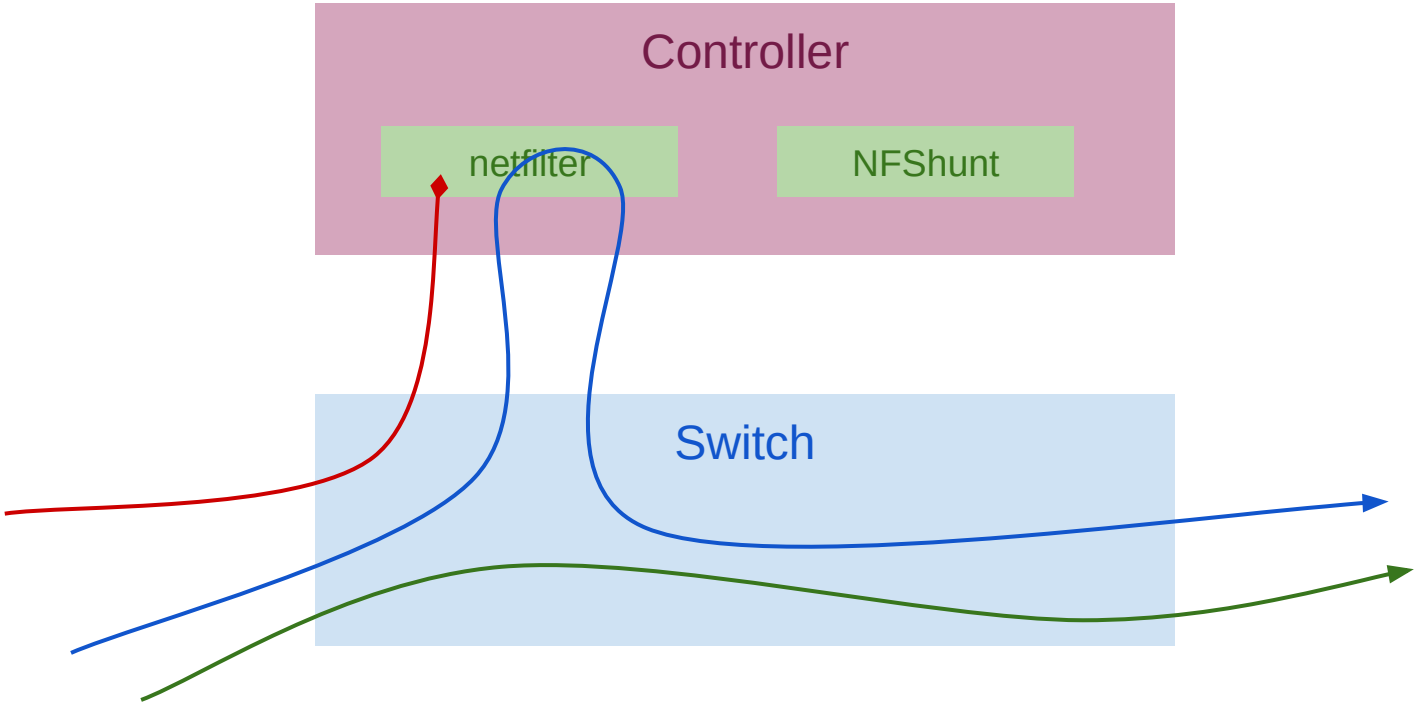
- Are they secure enough?
- Use a lot of flow table entries for an OpenFlow solution

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON
PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE

NFShunt!

- Made by Simeon Miteff at SANReN
- Hybrid Stateless-Stateful firewall
- Exploit long tail in network flow size
- Redirect to netfilter (or some other firewall) by default
- Large authorised flows redirected to bypass the firewall entirely

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON
PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE



TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE

Pros:

- Better security than ACLs
- Fewer OpenFlow rules than ACLs
- Line rate throughput for large flows
- SSH, HTTPS - no point in looking at more than the first couple of packets anyway
- Default drop actions can mitigate attacks against the firewall itself

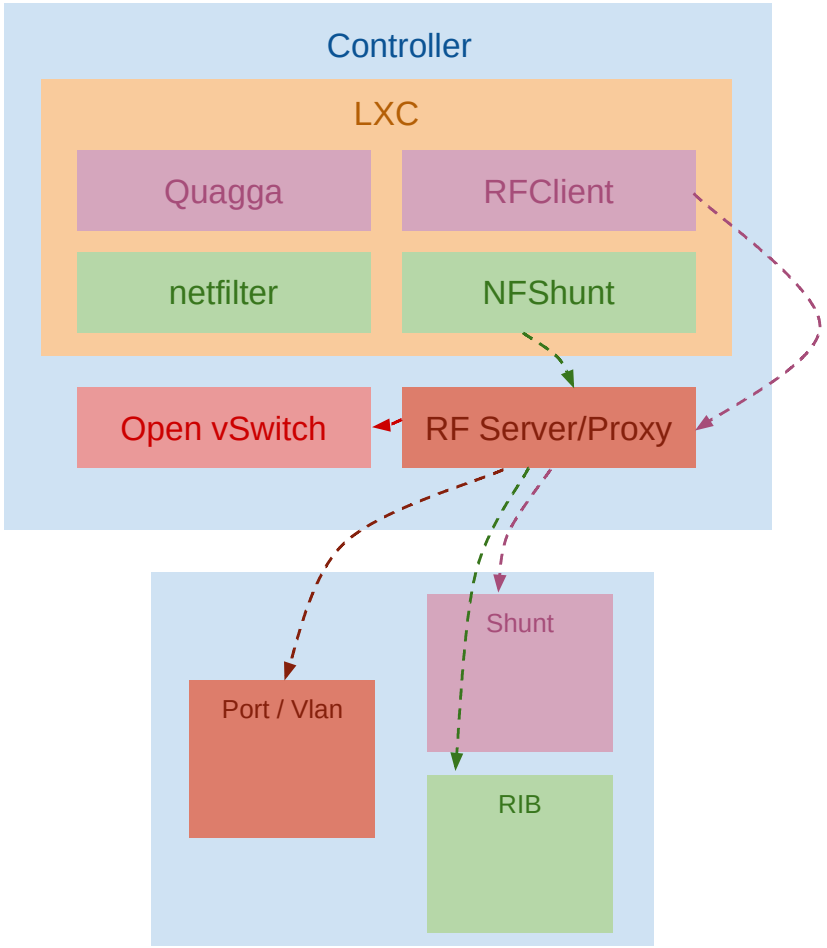
TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON
PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE

Cons:

- Less secure than a firewall
- Can’t match on TCP flags
- Can’t match on layer 7

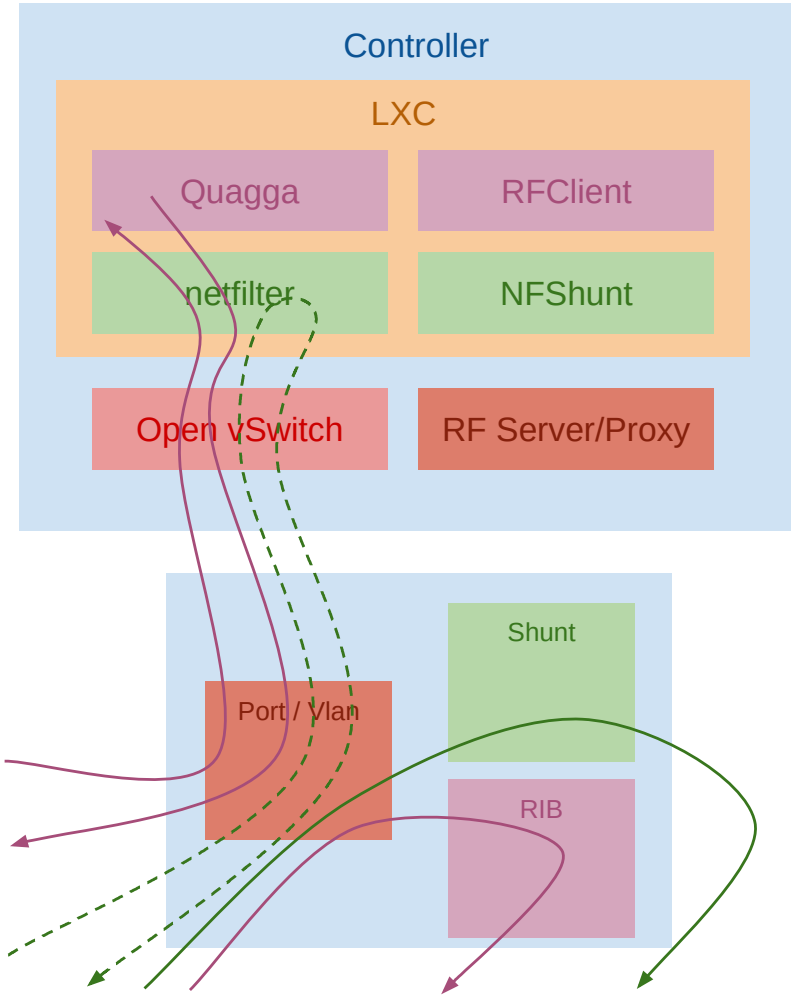
PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE
TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON

Plugging NFShunt into Vandervecken



PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE
TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

Plugging NFShunt into Vandervecken



PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE
TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON

Redirection vs Encapsulation

- Encapsulation is Ethernet over OpenFlow over TCP
- NFShunt uses redirection, RouteFlow uses encapsulation
- Encapsulation allows sending partial packets
- Encapsulation gives extra information:
  - Reason / Cookie / Table id
  - Match: In Port / Metadata

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON
PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE

RouteFlow redirection

- Need in port information on packets from datapath
- Need to know where to output packets from controller
- Use Vlan tags (or MPLS labels)

PICA8 OPEN NETWORKING
REANNZ
catalyst
IEEE
TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI VICTORIA UNIVERSITY OF WELLINGTON