Proofs of In-Line Functionality in SDN Networks

eResearch Conference, Queenstown
Matt Stevens
7th February 2016

What is SDN ?

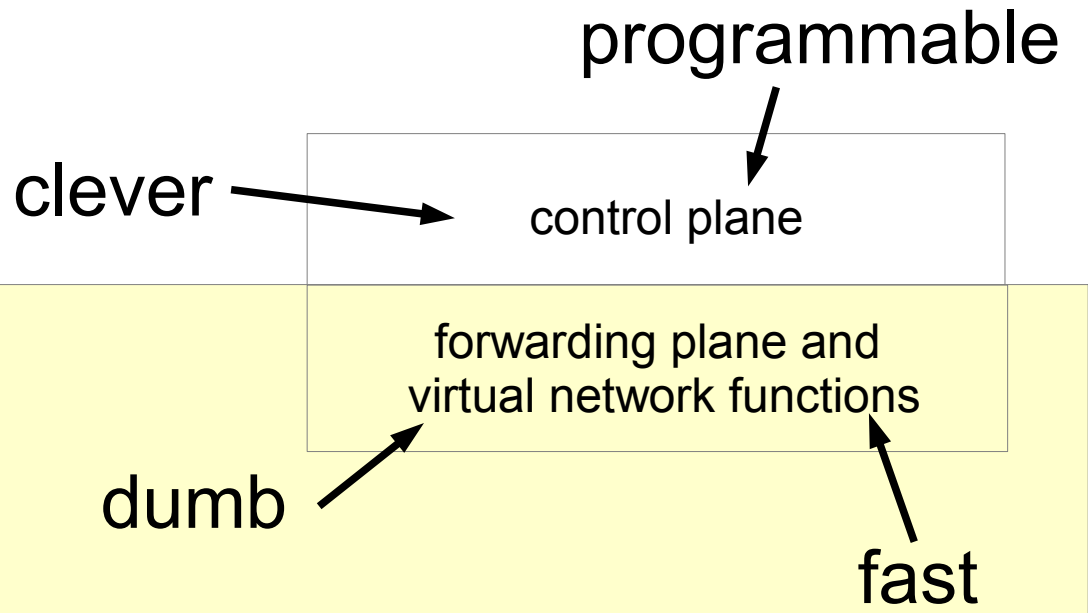
It is a network architecture that separates the control plane from the forwarding plane

It applies to Routers and Switches that provide Layer 2 and 3 routing protocols

In-line functionality may also benefit from using the control plane

<u>Key network benefits</u>

- Resource optimisation enabled by the centralised view and automation.
  {people, capital, infrastructure}
- Ease of introducing new technologies
  {experimentation, updating software, no provider lock-in}



"Across all network sizes, the number of middleboxes
is on par with the number of routers in a network!"
A Survey of Enterprise Middlebox Deployments, Sherry & Ratnasamy (2012)

What is NFV ?

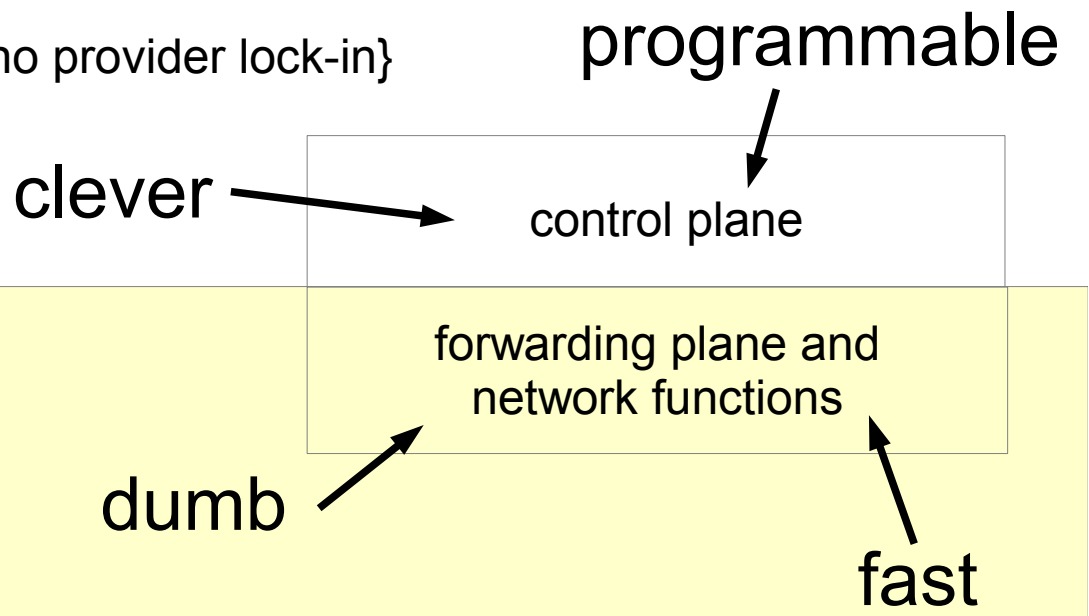
It is a network architecture that separates software from hardware using virtualization

Proprietary network hardware can be (and is) specialised for performance,
but it costs.

Generic hardware is slower but can achieve higher utility,
similar performance can be gained through parallelism

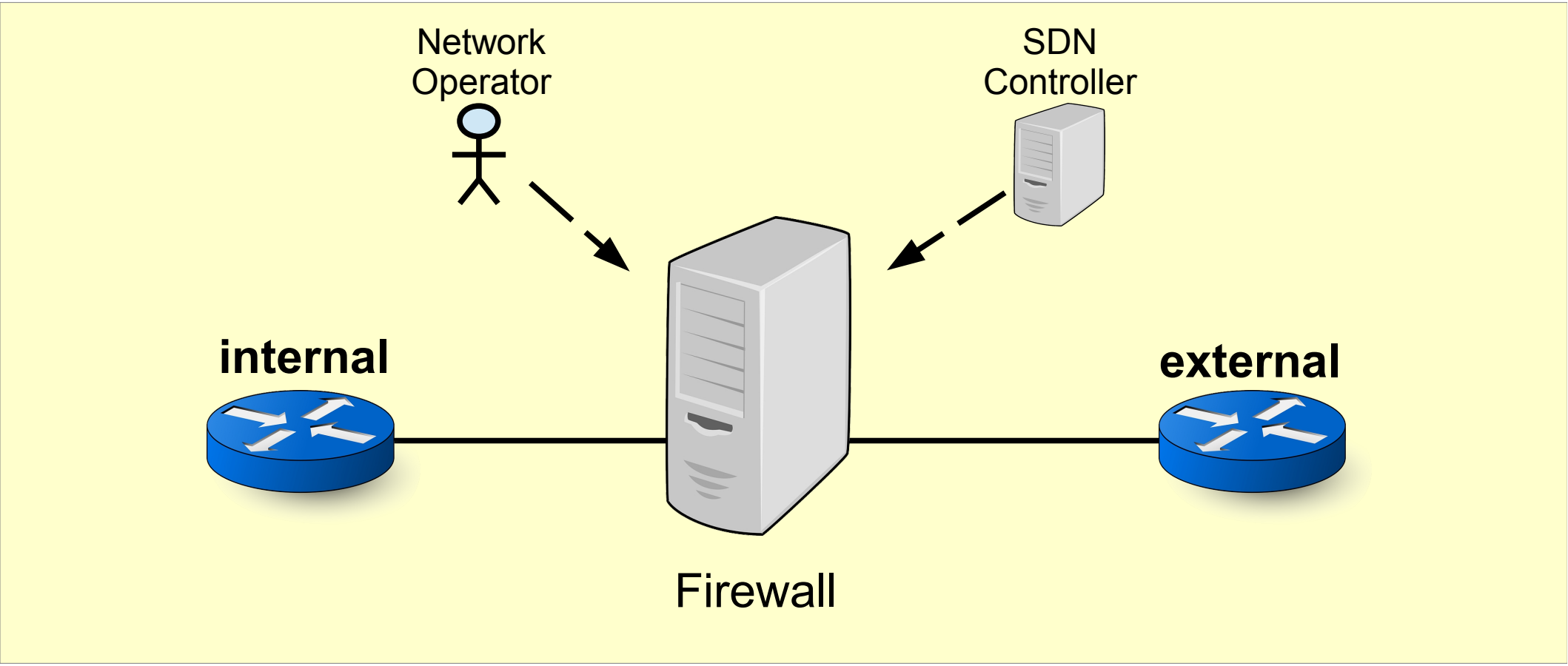
<u>Key network benefits</u>

- Resource optimisation when combined with a centralised view and automation.
  {people, capital, infrastructure}
- Ease of introducing new technologies
  {experimentation, updating software, no provider lock-in}



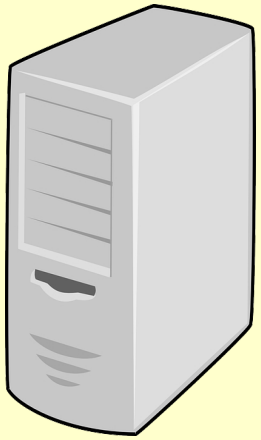
Open vSwitch
"purpose-built for use in virtualised environments."
Extending Networking into the Virtualization Layer, Pfaff *et al* (2009)

Firewall Middlebox as an In-Line Service

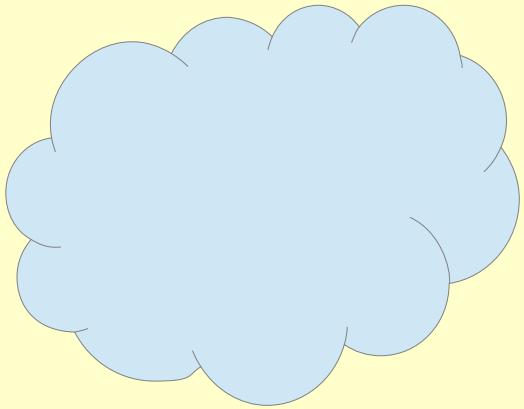


Operates on the packets it sees
Manages it's own FW state
Decoupled from all other elements in the network
Operates at line speed (unless DPI is required)
Needs limited ongoing attention from the controller

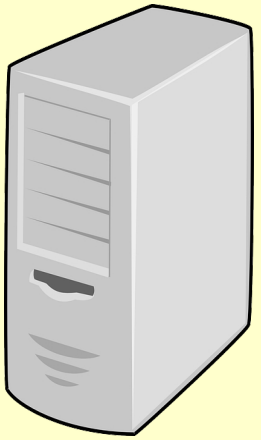
Implementing in-line services



Proprietary hardware and software



IaaS and SaaS in the cloud



Generic hardware with VMs or Containers

JUNIPER NETWORKS

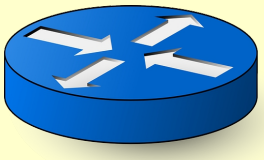
vgb drive

Spark Digital

docker

CISCO

f5

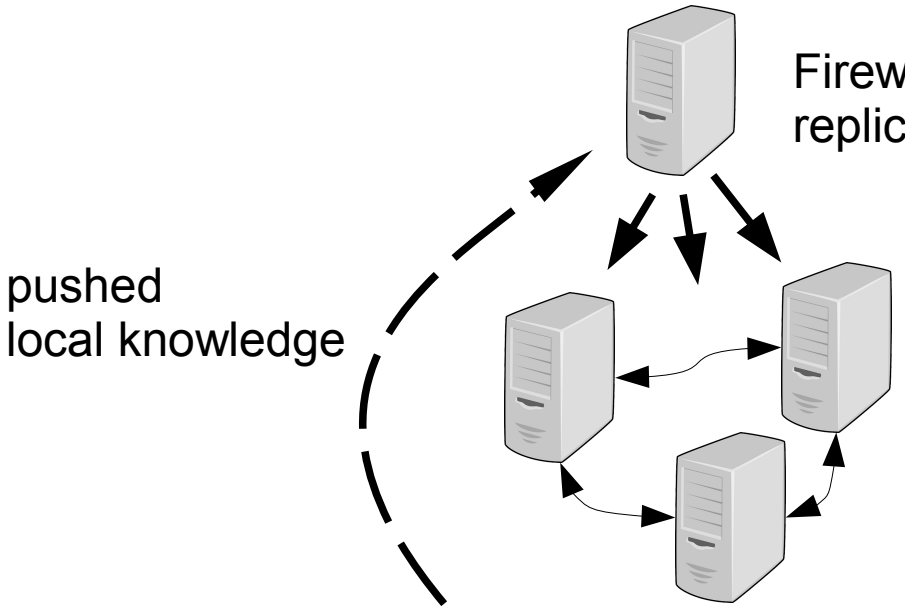


Generic Switches as state machines (ongoing research)

VirtualBox

SDN In-line Services – moving the algorithm off-line

(for example, FlowGuard 2014)



Firewall with ACL and session state, replicated on each controller.

pushed
local knowledge

Logically centralised SDN Controller.

Replicated for reliability in event of controller failure or network partitioning.

internal

external

SDN 'dumb' switch

Solves 'problems' the SDN community perceives in in-line services

Global and Local Knowledge in SDN. Stevens, Ng, Welch & Streader (2015)
Includes a survey of 15 recent (2014+) SDN survey papers on SDN

Network Invariants

Provable global routing properties

- No loops
- No black holes
- Host reachability

Optimisable Network properties

- Power consumption
- Labour costs / human error
- Latency
- Hardware / capital costs
- Failure recovery time
- Software updating
- Flow capacity
- Resilience under network stress

The Network Proving Problem

Provable global routing properties

- No loops
- No black holes
- Host reachability

Off-line services may prompt
frequent off-line proofs of the network
for example dynamic firewall changes, directly impact host reachability

In-line services make proving network properties difficult

- Dynamically **re-route** packets
- Dynamically **re-write** packets

What if?

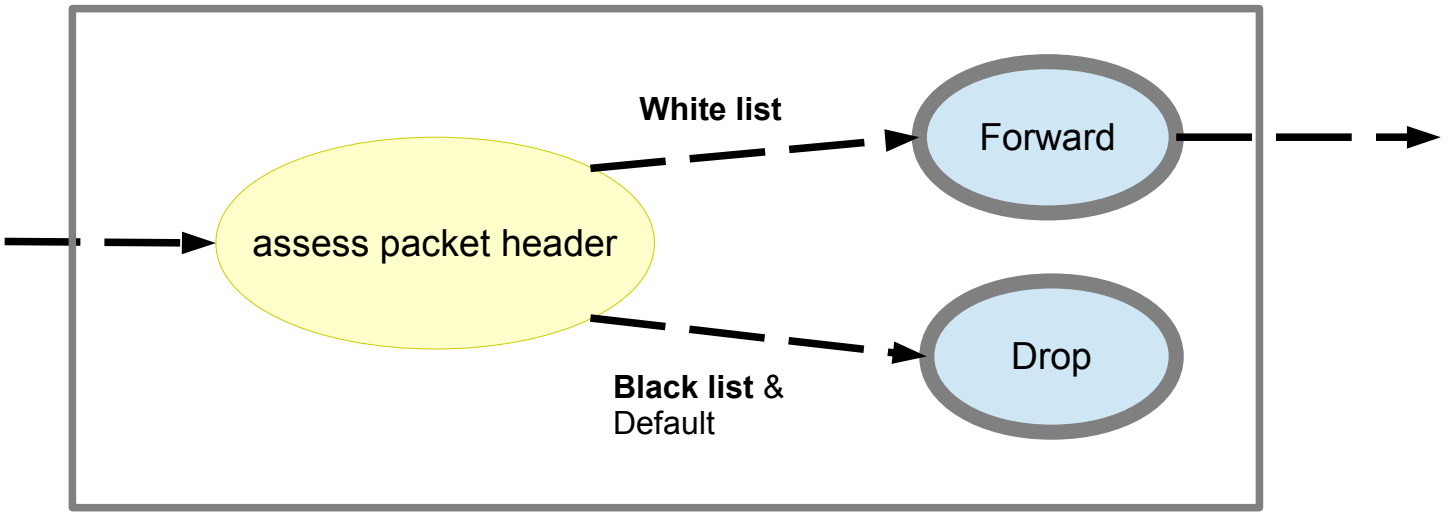
Can in-line functionality

- be defined in terms of network properties?
- ensure no surprises?

Research Goals

1. Contribute an implementation independent model of a class of in-line network service that provides provable deterministic properties.
2. Create a test harness that enables the testing of any implementations of this class of in-line service.
3. Use the abstraction of this class of in-line service to simplify proving network properties.

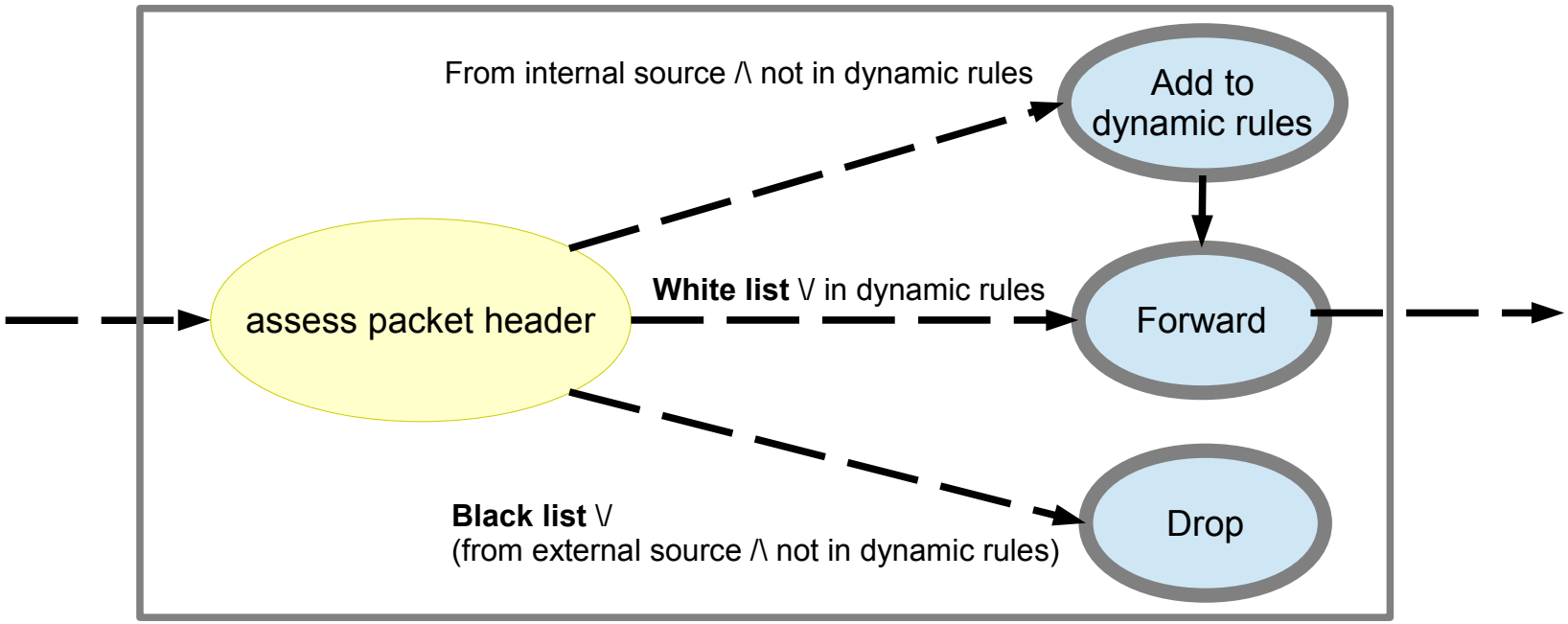
A stateless Firewall



NB: Trusted and Dangerous rules do not expire

ACL **White list** and **Black list** are defined by the controller.
Firewall **placement** is defined by the controller.

A stateful Firewall



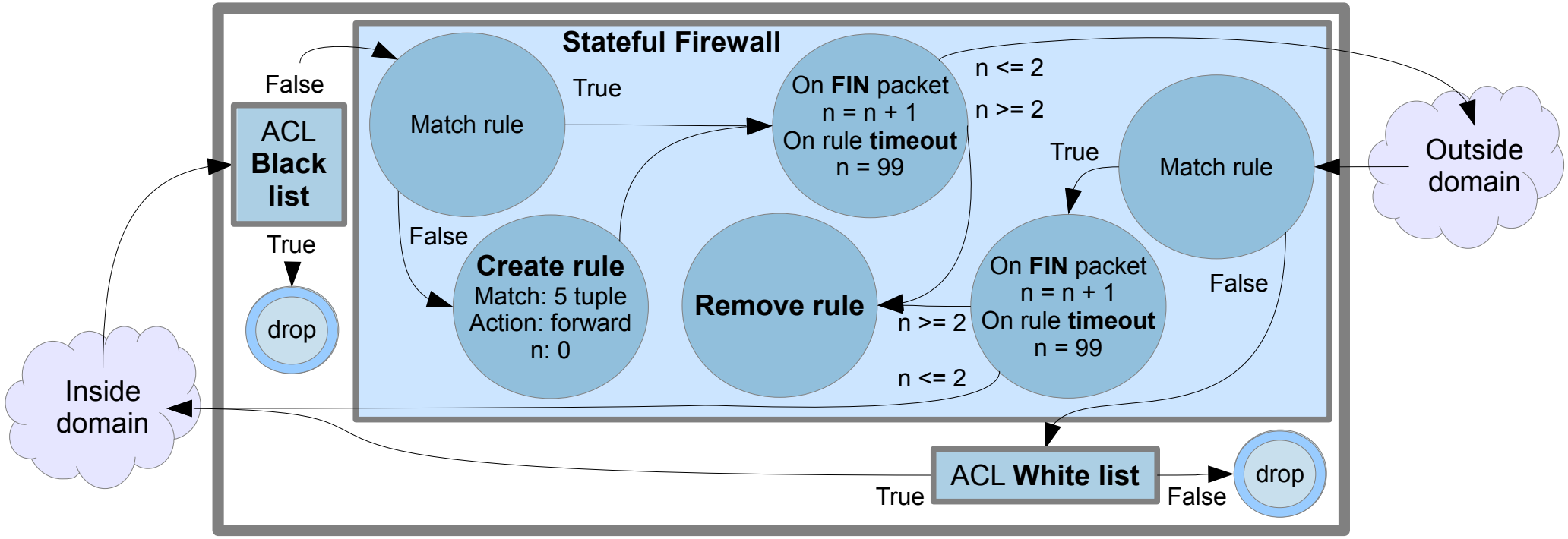
NB: dynamic rules expire using a timeout value
or, for example, on a TCP FIN packet.

ACL **White list** and **Black list** are defined by the controller.
Firewall **placement** is defined by the controller.

A stateful Firewall

that ensures no surprises

caveat – we may yet be surprised!



ACL **White list** and **Black list** are defined by the controller.
Firewall **placement** is defined by the controller.

For example, this model assumes TCP ACK packets are harmless and allows access both ways.
Surprise! ---> this may facilitate data leaks

Test Hypothesis

In-line firewalls may satisfy black box tests while firewalls implemented off-line may fail due to use of off-line state.

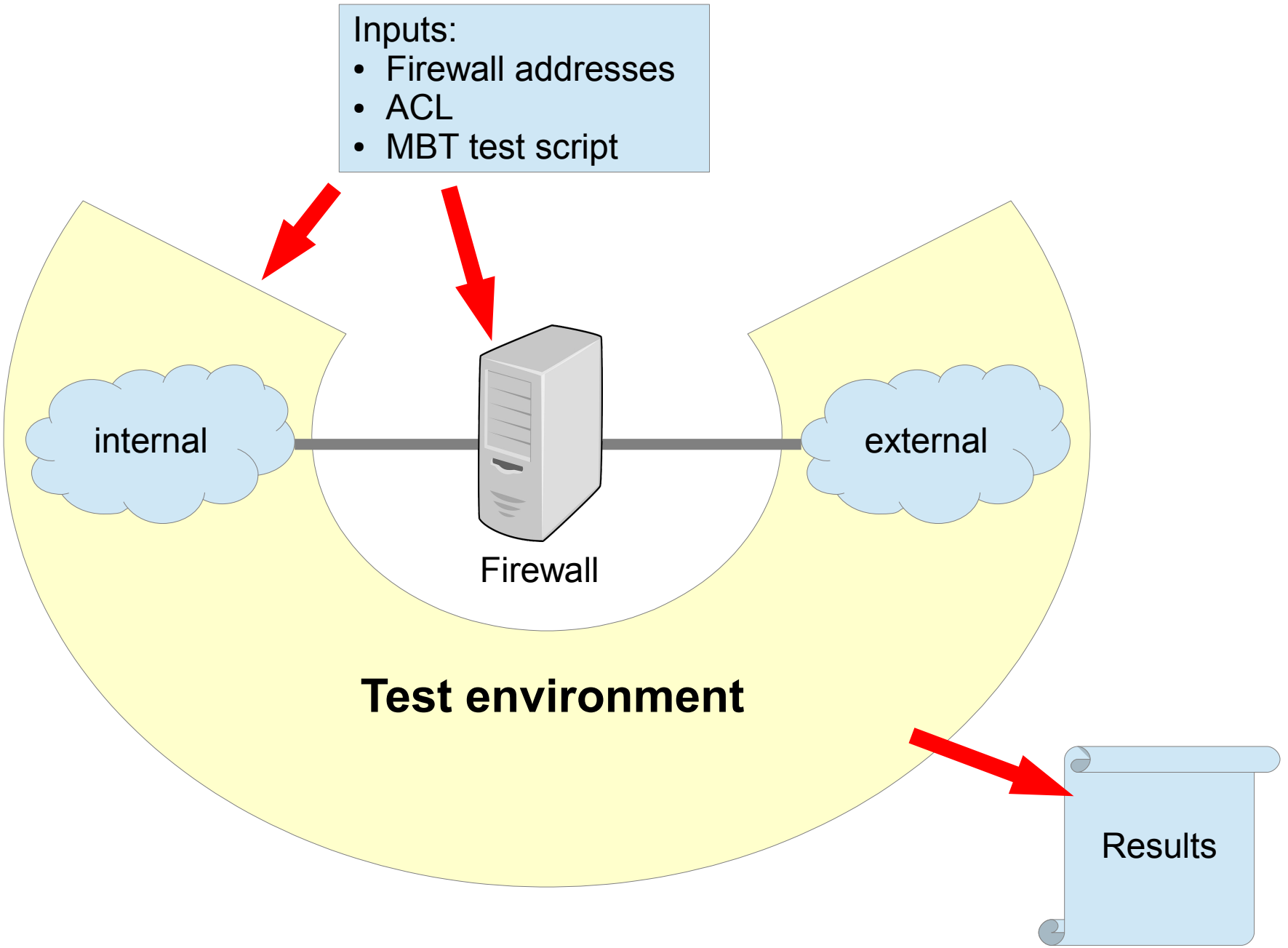
Expect to see examples of the following in SDN Firewalls;

- **Adversaries able to maintain perpetual TCP sessions**
  End hosts believing TCP sessions are finished, while the FW thinks they are open

- **Adversaries able to send data packets from internal to external host.**
  Allowing all FIN and ACK packets to exit the internal domain

- **Adversaries able to conduct DDOS attacks directly on controller.**
  TCP SYN and/or FIN packets are sent directly to the controller for resolution

Test Harness



Thank you

Looking for in-line services

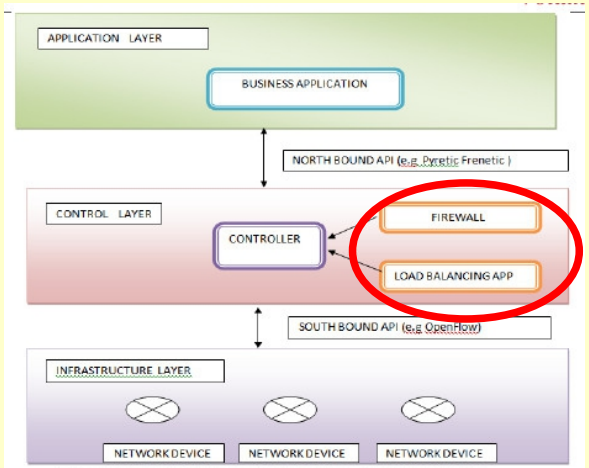


Fig 1: Software Defined Networking Architecture [2]

Ranjan etal. 2014. A survey of past present and future of software defined networking. *International Journal.*

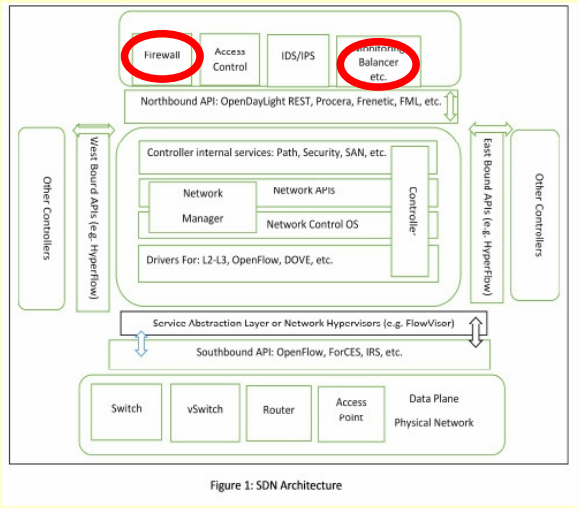


Figure 1: SDN Architecture

Alsmadi etal. 2015. Security of software defined networks: A survey. *Computers and Security.*

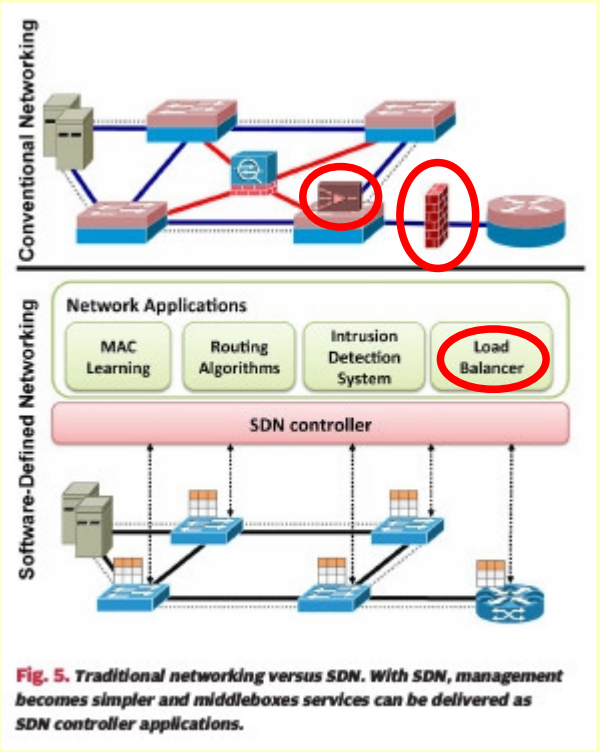


Fig. 5. ***Traditional networking versus SDN. With SDN, management becomes simpler and middleboxes services can be delivered as SDN controller applications.***

Kreutz etal. 2015. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE.*

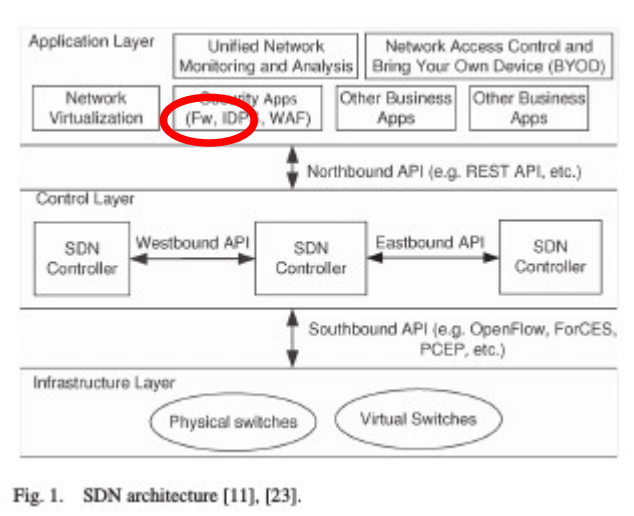
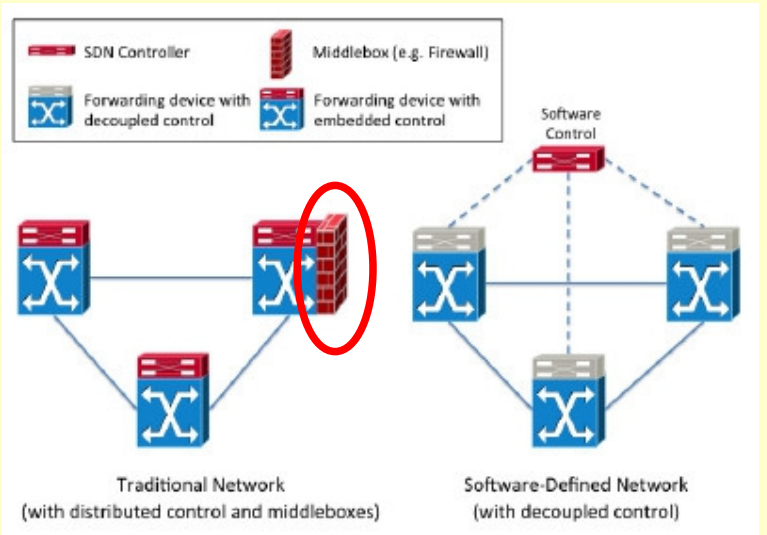


Fig. 1. SDN architecture [11], [23].

Jarraya etal. 2014. A survey and layered taxonomy of software-defined networking. *Communications Surveys and Tutorials, IEEE.*

Finding it in or above the control plane – in 15 recent surveys of SDN research.

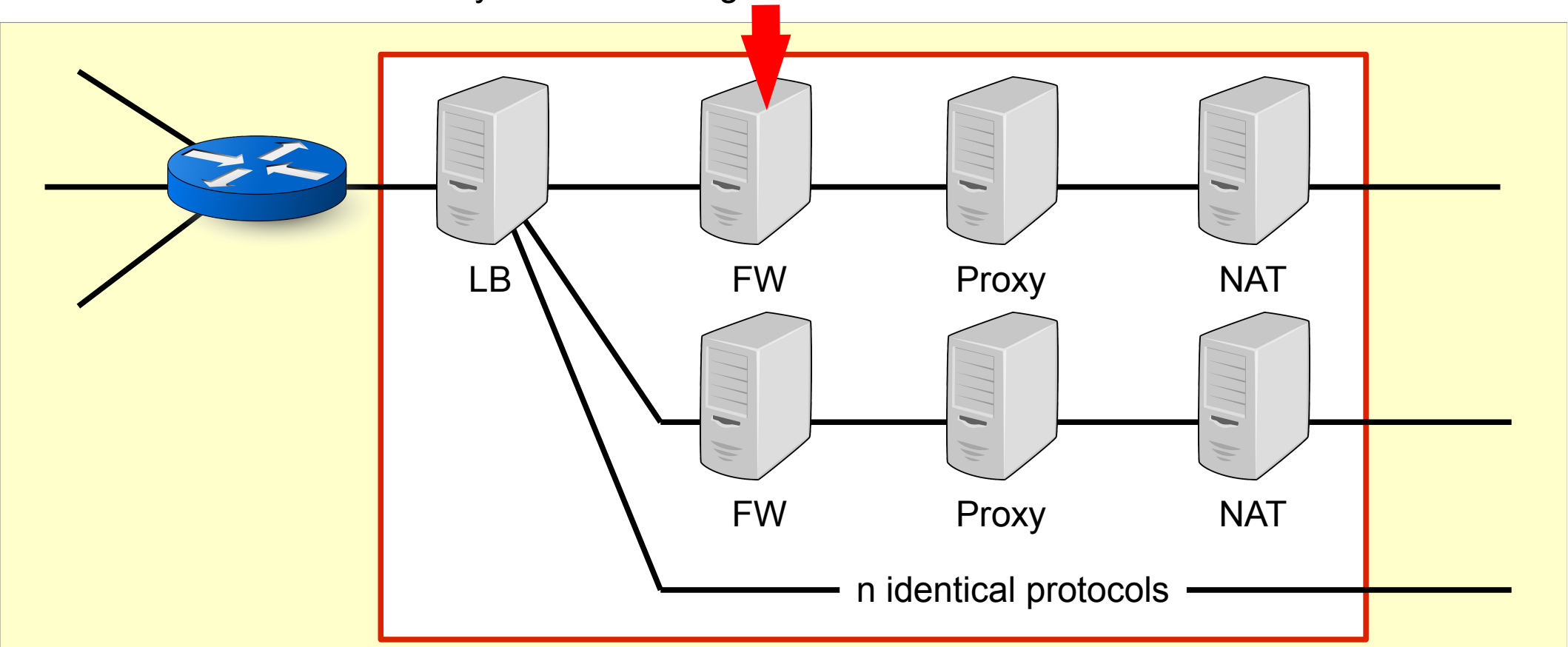


Nunes etal. 2014. A survey of software-defined networking: Past present and future of programmable networks. *Communications Surveys and Tutorials, IEEE>*

High-end In-line Firewall

Defeats reconnaissance and attack by multiple classes of in-line service working in concert

This talk considers only the Firewall algorithm.



See; F5 Firewall