

SSH Cure

Implementatie en ervaringen

NLNOG-dag 2014, Amsterdam

Luuk Hendriks
Design and Analysis of Communication Systems

UNIVERSITY OF TWENTE.

whois

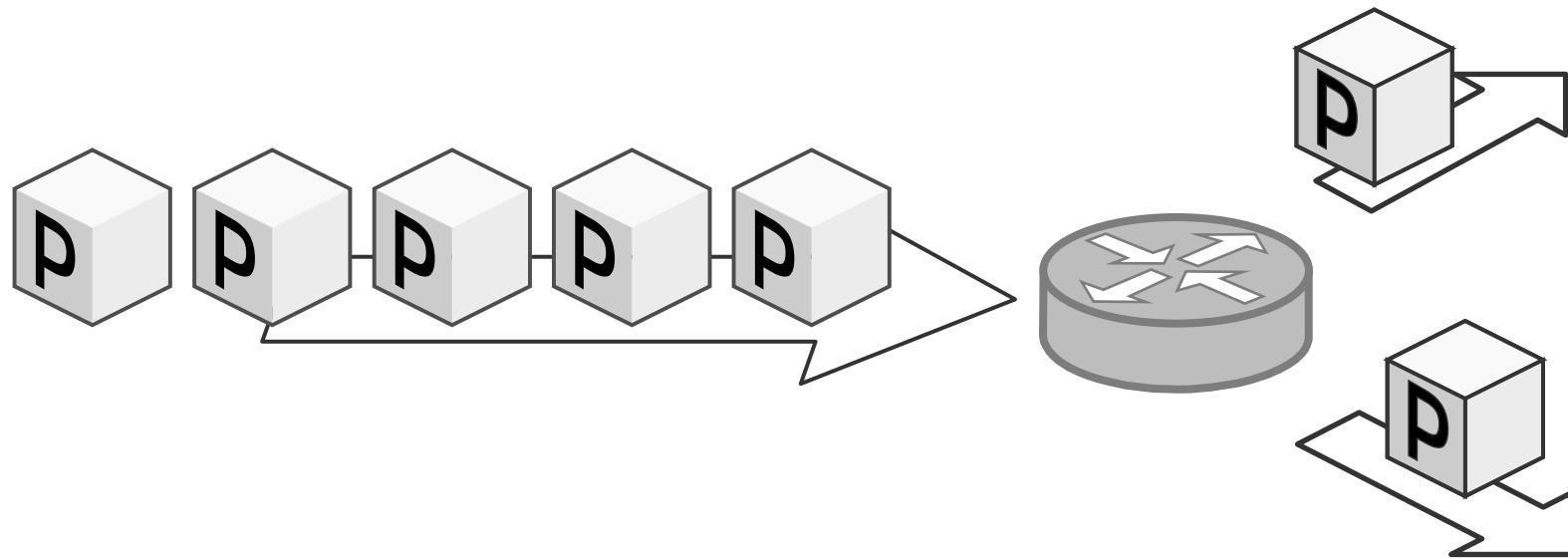
**Luuk Hendriks, sinds april 2014
promovendus Universiteit Twente,
geïnteresseerd in Network Security**

Thuisbrouwer & platenverzamelaar

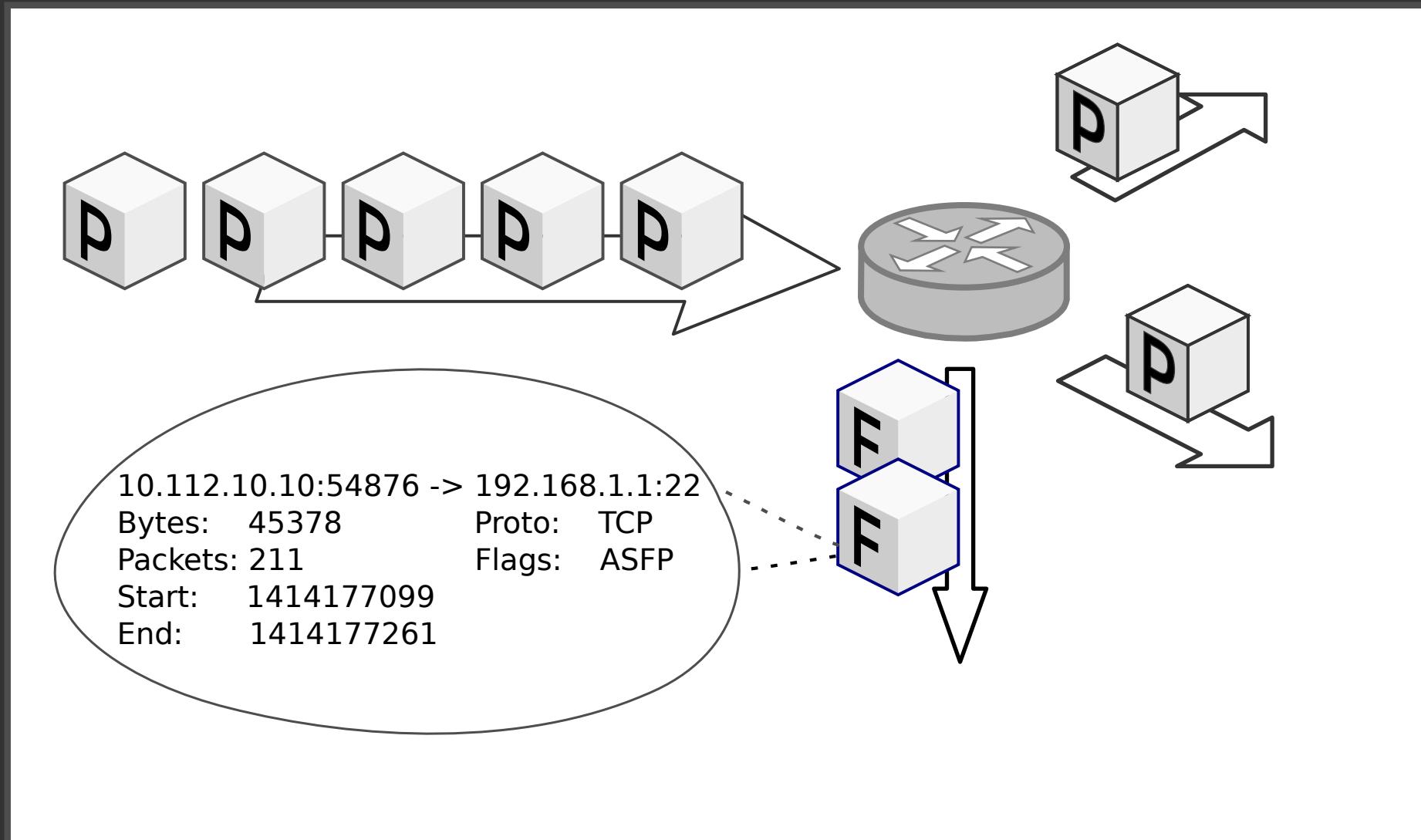
SSHCure is een **flow-based** intrusion detection system

Wat weten we na drie jaar ontwikkeling?
Voordelen, **valkuilen**, lessen
in theorie, en in **praktijk**.

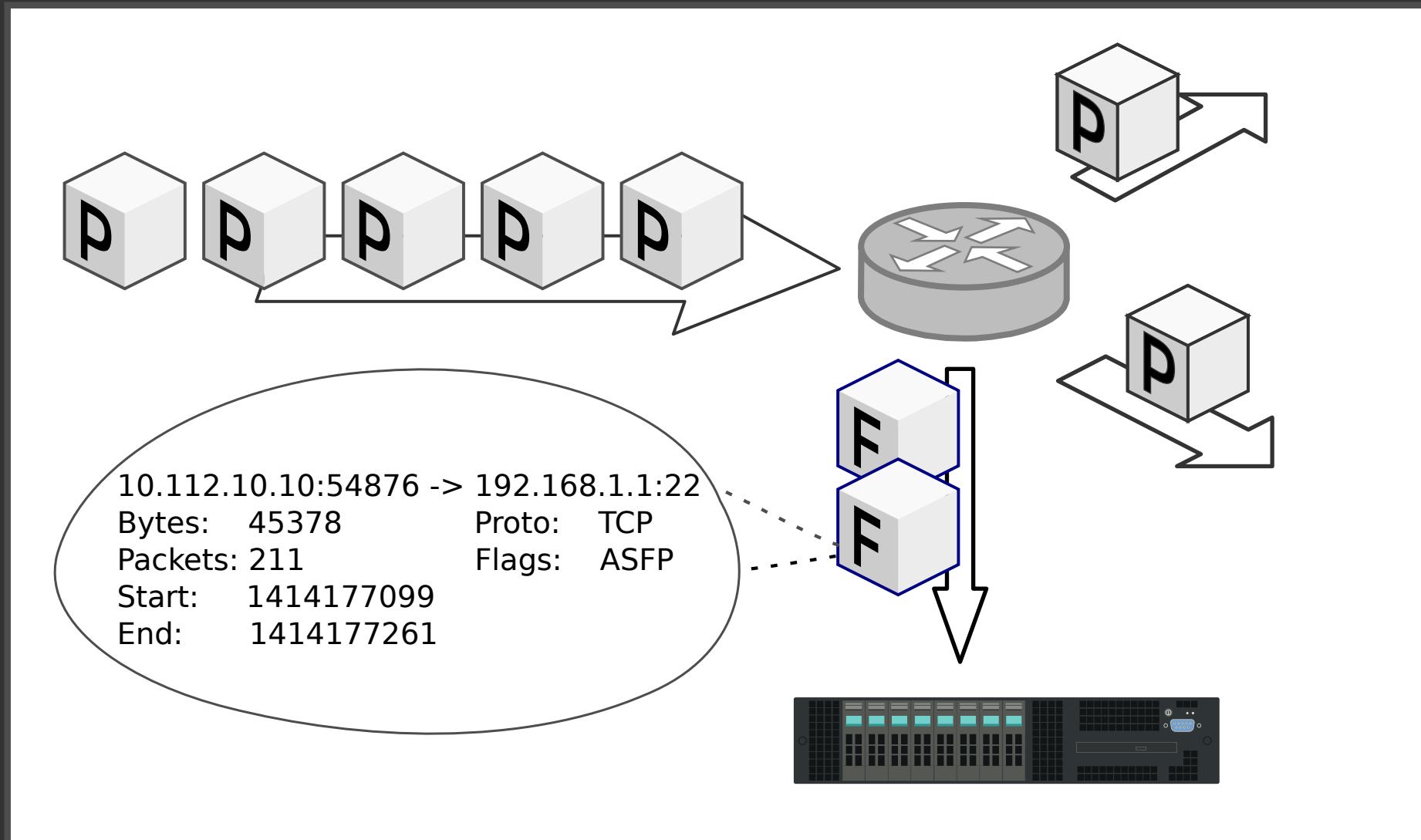
(Net)Flow 101



(Net)Flow 101



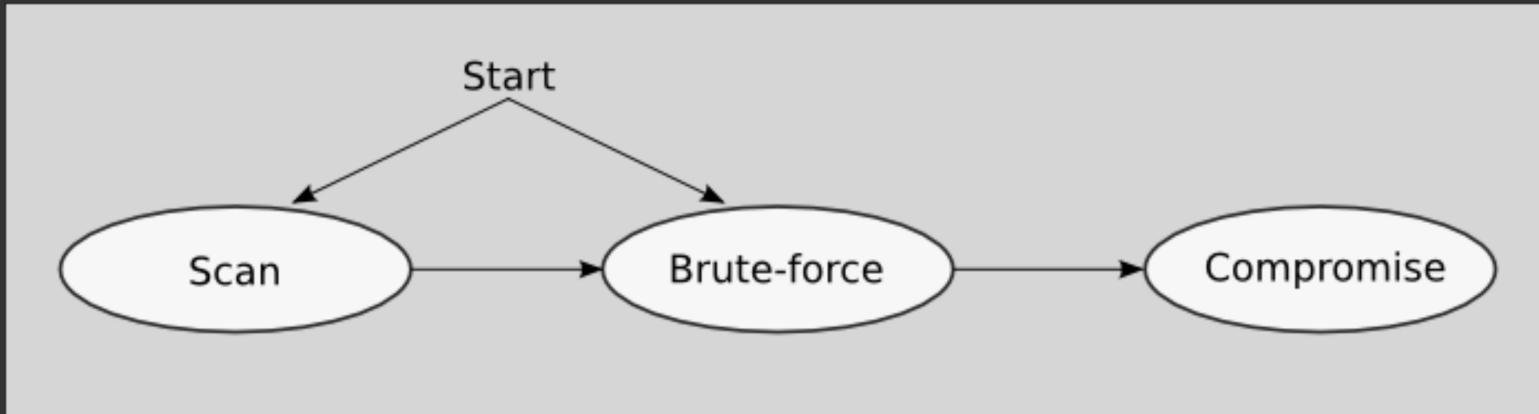
(Net)Flow 101



SSHCure is gebaseerd op een **fase-model**[1]:
scan, brute-force, compromise

Onderscheid en overgang tussen deze fasen
kan op basis van het aantal
Packets Per Flow (PPF)

[1]: Anna Sperotto, “Flow-based Intrusion Detection”, 2010



Puur PPF-based aanpak was
veelbelovend, echter met
te veel false positives. Waarom?

Valkuil 1: flows

Aggregatie van packets

==

informatieverlies

==

schaalbaar

Inter-arrival times? Retransmissions?

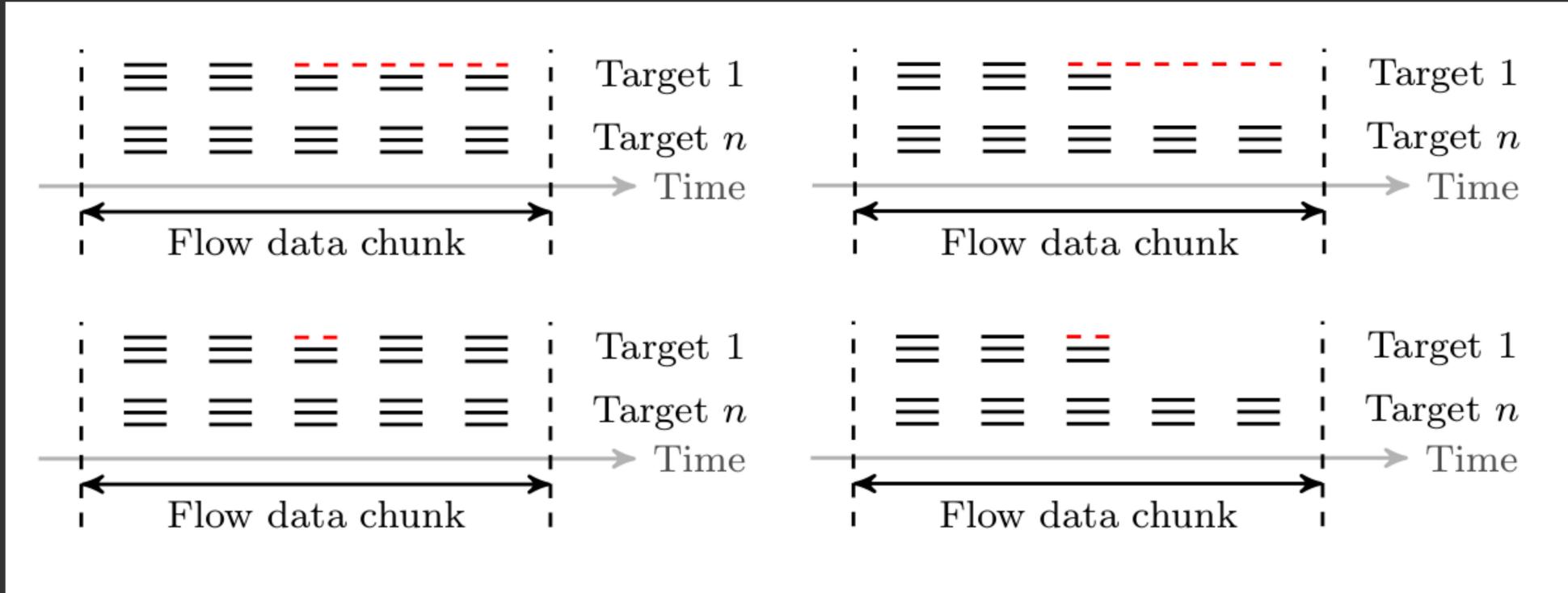
Detectie gebaseerd op PPF-afwijkingen in L5
is onderhevig aan fenomenen
in L3/L4.

Retransmissions uit China, fail2ban, ...

Redeneren op hoog niveau
vereist alsnog kennis van laag niveau

Uitgebreide analyse van
zowel **attack tools**
als de OpenSSH **daemon**
resulteert in:

- veel verrassingen
- vier scenario's



“SSH Compromise Detection using NetFlow/IPFIX”

R. Hofstede, L. Hendriks, A. Sperotto, A. Pras
In:
ACM SIGCOMM Computer Communication Review
#44, Oktober 2014

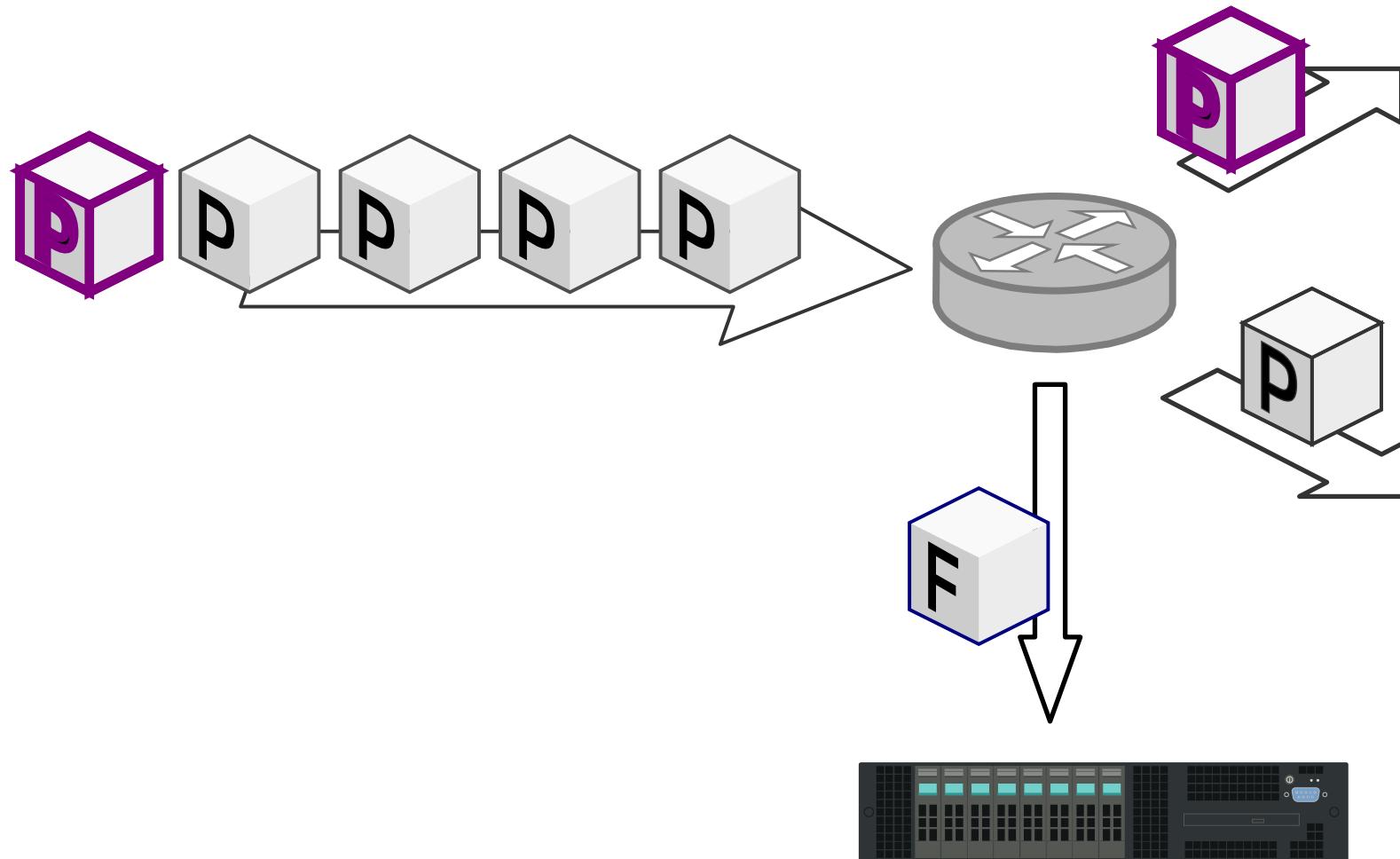
Valkuil 2: hardware

Alle apparaten doen NetFlow, sommige
doen alleen meer NetFlow dan anderen.

UDP flags ?!
Flows van 6 maanden oud ??!

Sampling ?

1:5 sampling



tail ~/notes/nlnog2014.txt

- Verlies van details inherent
- Sampling maakt dit mogelijk erger
- Veel verschil in kwaliteit hardware
- Toepasbaarheid verschilt per scenario
(accounting vs forensics)

SSH CURE

SSHCure is een plugin voor NfSen:
Front-end in PHP
Back-end in Perl

Flow-informatie wordt gelezen door
`nfdump`

Nfdump kent `geen concurrency`

~~use threads;~~

Concurrency in SSHCure middels
io::async

Niet multi-threaded, maar
asynchronous, event-driven

Conventionele systemen detecteren
aanvallen;

Wij doen **compromise-detectie**.
Volledig flow-based.

*“Our rule no. 1:
it's not about what goes into our network,
it's about **what goes out.**”*

- NREN operator @ TNC

Flow-based systemen zijn
richting-agnostisch.

Bij detectie van *incoming attacks*,
gratis detectie van *outgoing attacks*

Dashboard

Incoming

Outgoing

Dashboard

Incoming

Outgoing

SSH**Cure** 3.0

Attacks

Scan Brute-force Compromise

Day Week Month



Incoming attacks

Phases	Active	Attacker	Start time	Targets
			Thu. Oct 23, 2014 17:13	926
			Thu. Oct 23, 2014 10:40	4071
			Thu. Oct 23, 2014 06:03	28
			Wed. Oct 22, 2014 22:01	13
			Wed. Oct 22, 2014 20:47	37306

Top targets - Compromise

Target	Attacks	Compromises
		No data available...

Free, open source:

<https://github.com/SSHCure/SSHCure>

NfSen-plugin, *nix + BSD ondersteuning

Phases	Active	Attacker	Start time	Targets
			Thu. Oct 23, 2014 17:13	926
			Thu. Oct 23, 2014 10:40	40781
			Thu. Oct 23, 2014 06:03	28
			Wed. Oct 22, 2014 22:01	13
			Wed. Oct 22, 2014 20:47	37306

Target	Attacks	Compromises
		No data available...

Search

Status

Help

Settings

cat ~ / sshcure / TODO

Distributed / stealthy attacks ?

IPFIX Information Elements ?

IPv6-'ready' ?

Evaluatie van SSHCure 3.0

SSHCure

Implementatie en ervaringen

NLNOG-dag 2014, Amsterdam

Luuk Hendriks

luuk.hendriks@utwente.nl

IRC/GitHub: DRiKE

UNIVERSITY OF TWENTE.