NuFW

The identity-based firewall
or
Why using Netfilter is cool !

Eric Leblond, eric@inl.fr

Plan

- Introduction
- NuFW's genesis
- Presentation of the algorithm
- NuFW and nfnetlink
- What's next
- Conclusion

In the beginning was

- 2001, the raise of Netfilter:
  - Statefull filtering
  - Modularity
  - Protocol helper
- Some interactions with userspace :
  - Iptables: the well known configuration tool
  - Userspace decision: ip_queue (-j QUEUE)
  - ULOG : avanced logging
    - Text based and binary output
    - Database output

A time of great struggle and heroic deeds

- Nefilter connection tracking:
  - Table of known connections
  - Capability to decide on a packet following
    - Presence in the table
    - State in the table
- See (or Remind) Pablo's conference for details

Welcome in the real world

- Firewall are real world object
  - They are deployed in concrete enterprise/organisation
  - To implement security policy
- Security policy are made by human
  - To control access to resources (limit access from internet)
  - By system (control access between servers)
  - And humans (control user access to resources)

I'm not a number

- Firewall were IP filter
  - Filtering following header of packets
  - Or in some case
    - Harware header
    - content
- They had no visibility on users
  - Unable to control access per user
  - Without assuming IP == User

Houston, there is a problem

- IP packets does not contain any user related information
  - Headers are totally user-free
  - Only content may have this information
- Supplementary method is needed
  - Protocol modification
  - External association

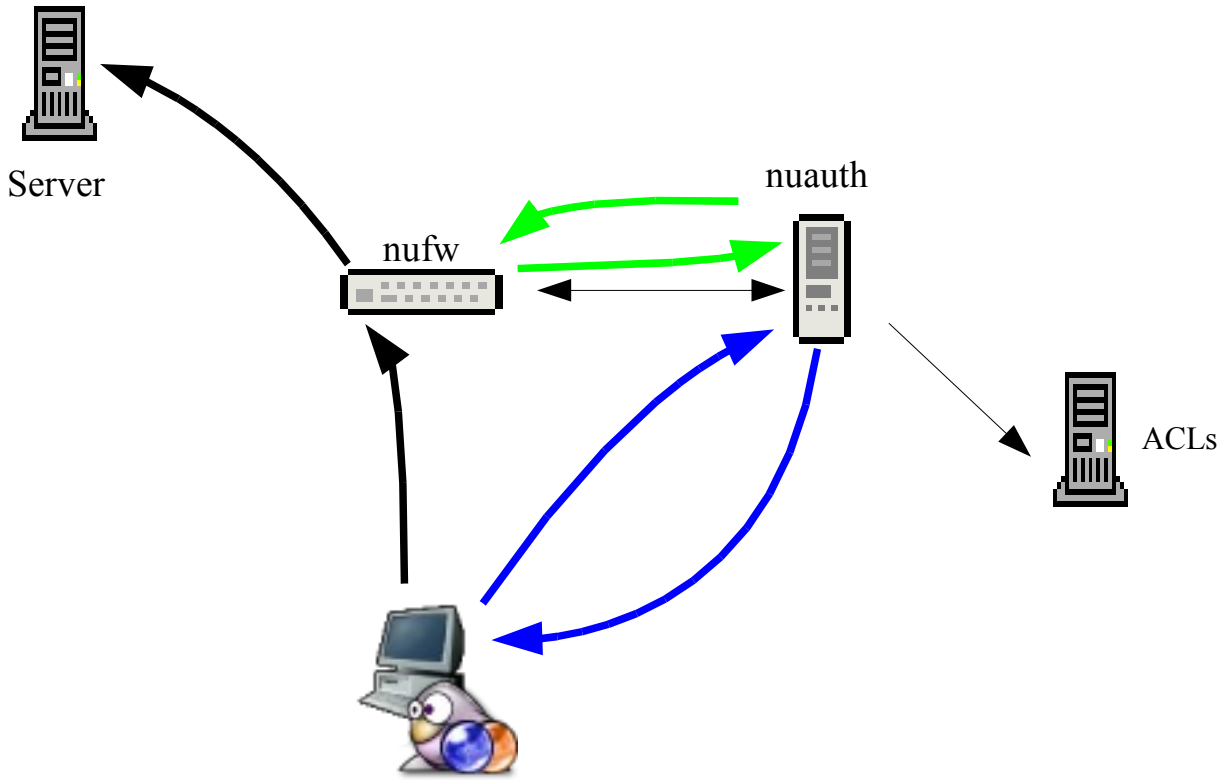
We're under attack

- Basic^W bad idea: IP == User
  - Association via external mechanism
  - Don't work on multiuser system
- Lot of attacks:
  - Spoofing (arp or IP)
  - Time attack

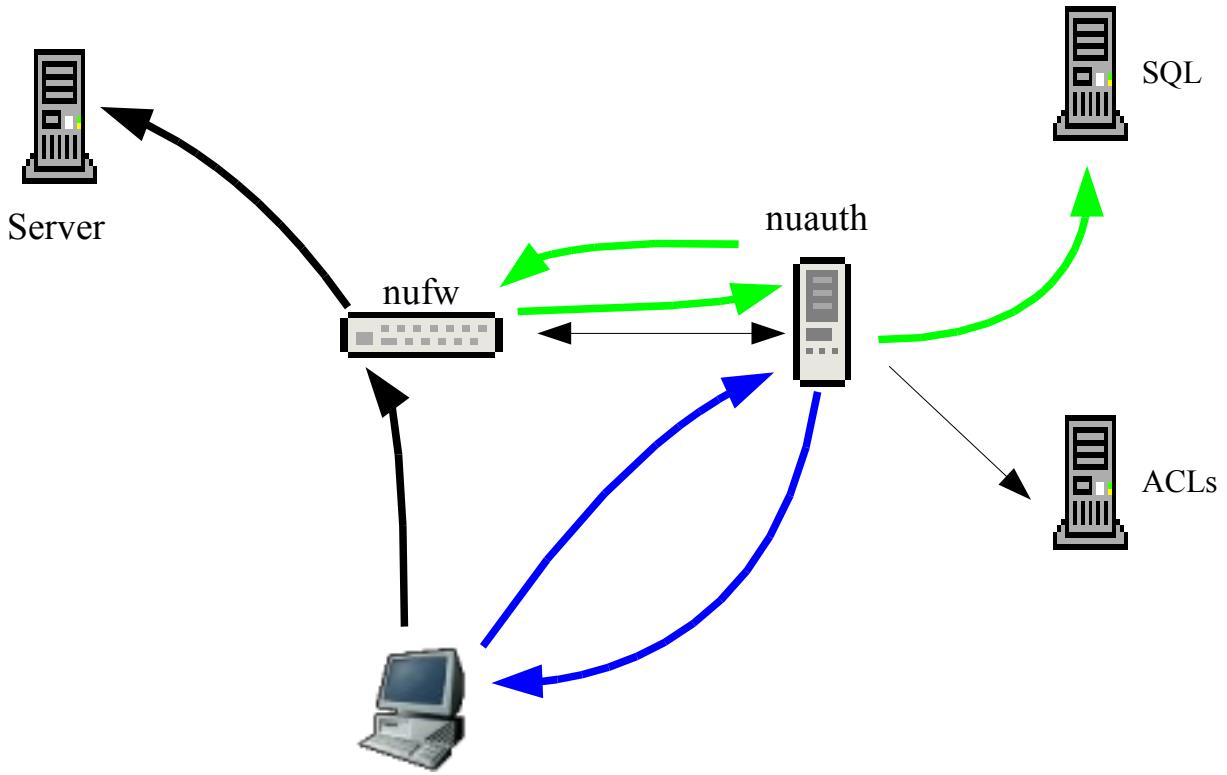
On the way to Babylon

- User query are connection based
  - In protocol way for TCP
  - More globally in the sens of Netfilter
- A priori brings no security
  - Time based attack
- Need A Posteriori authentication

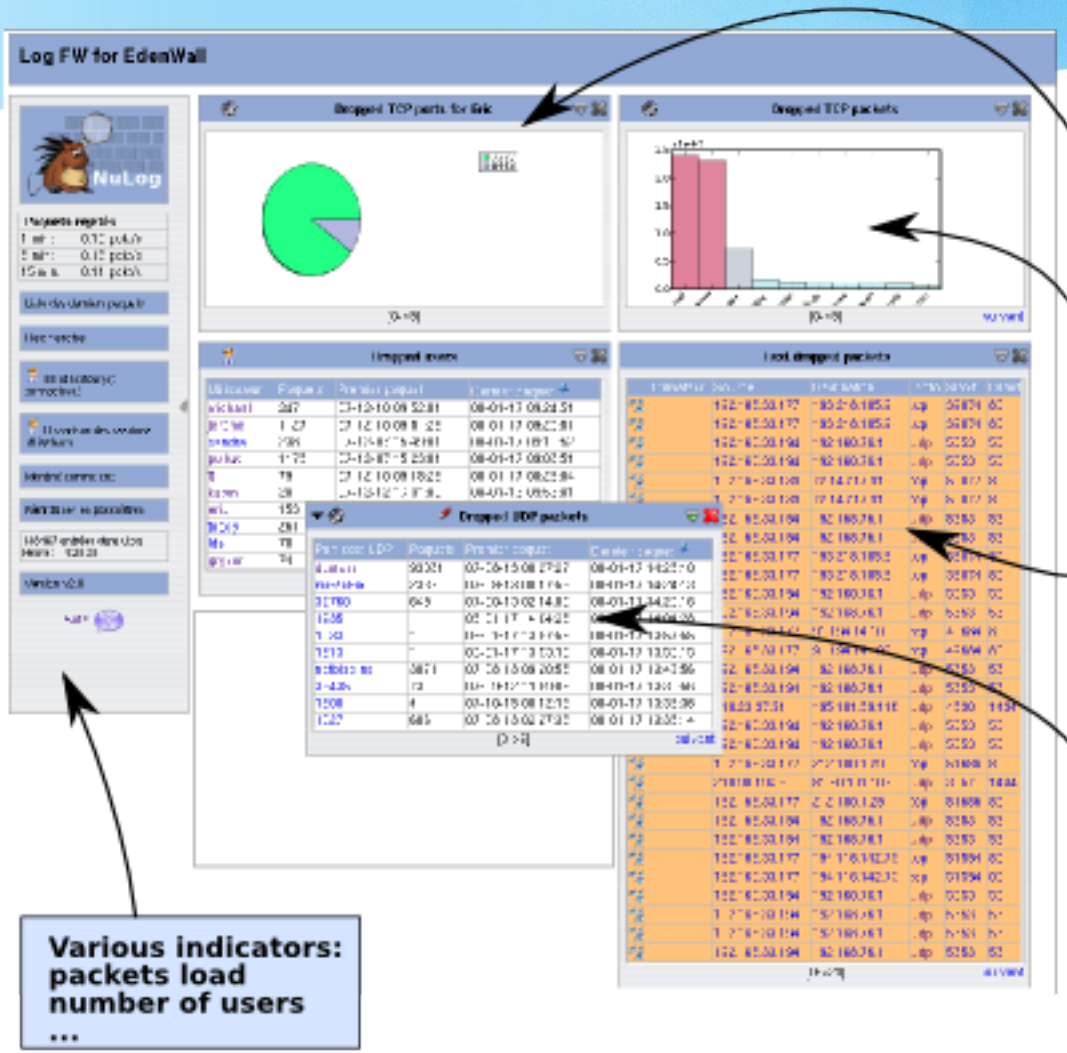
I'm doing it my way



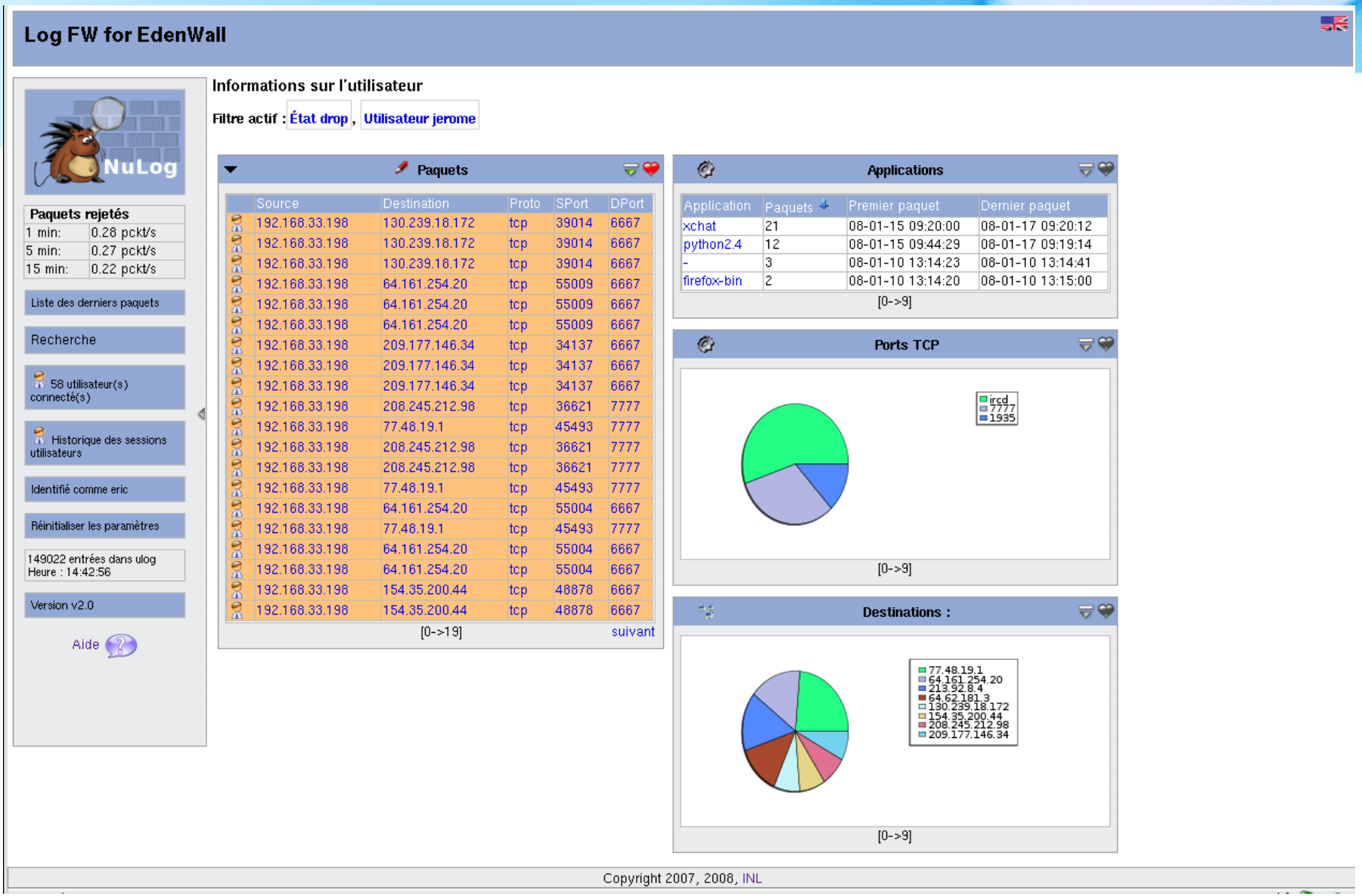
Bridget Jone's Diary



Bridget Jone's Diary



Bridget Jone's Diary

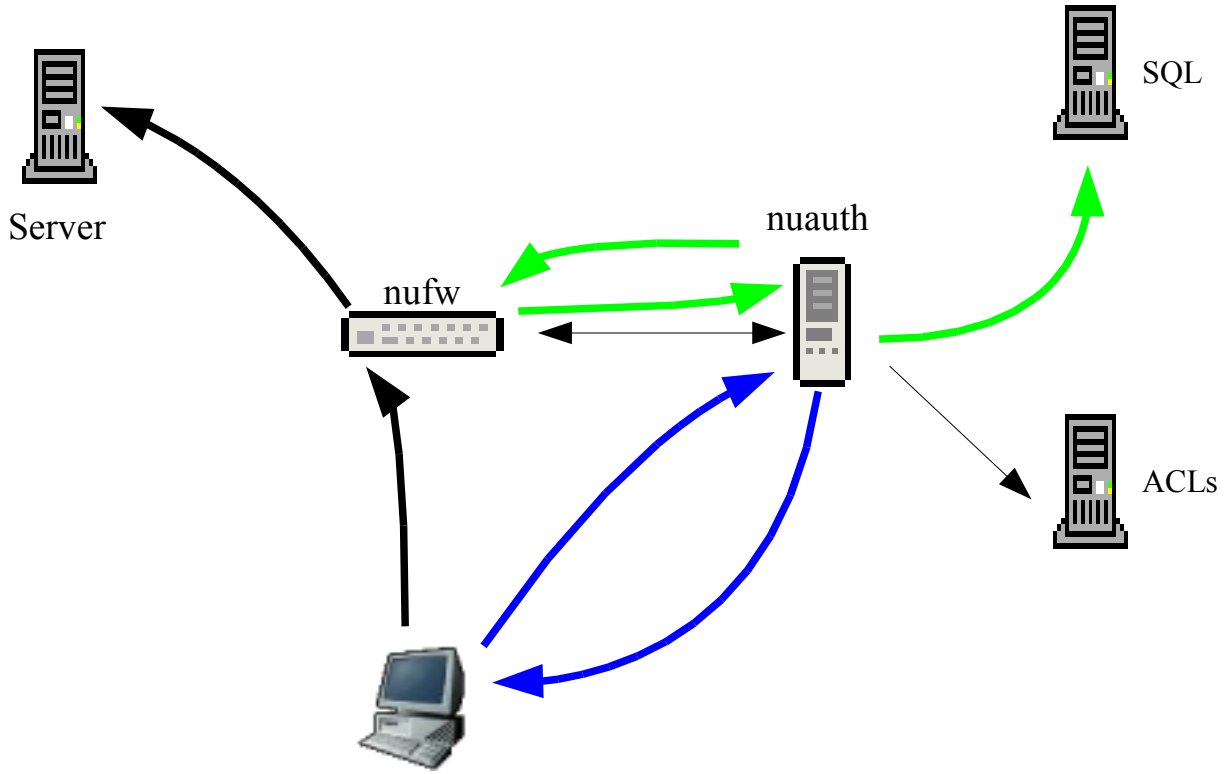


Let the police do its job

- Sysadmin are too busy
- Let human ressource manage the firewall
  - Direct link with directory
  - Integrated with IAM process
- Link filtering policy with the users/groups
  - Place in company will define user authorization
  - Employee will loose all rights when fired

We were expecting you Mr Bond

- Single Sign On



Supersize me

- NuFW is flow based
  - Connection is linked with user
  - Connection property can be set with user property
- Quality Of Service:
  - Can be per user
  - Can be on any arbitrary criterias
    - Application
    - OS
    - User groups

One ring to rule them all

- Working with SIM/IDS:
  - NuFW is strict (not regexp based)
  - HIDS sees information NuFW does not.
- Combining forces:
  - Suspicious behaviour:
    - User Martin logs on a ssh server as user Robert
  - Correlation:
    - Robert's account was hijacked by Martin

You say you want a Revolution

- Netfilter revolution in 2.6.14
  - Fight against lack of interaction
  - Centralize messaging system
- Nfnetlink
  - Multiplexing messages over netlink
  - Multiple subsystems
    - libnetfilter_log
    - libnetfilter_conntrack
    - libnetfilter_queue

It's my life

- Conntrack event gives information
  - At important step in the life of connection
    - Start
    - Establishement
    - Update
    - Destroy
- Following each connection individually with
  - Accounting
  - Application

Killing in the name of

- Connection destruction
  - Destroy any connection from conntrack
  - Block all subsequent packets from connection
- Time based filtering
  - Store destruction information on userspace
  - Kill them when their time has come
- BOFH module
  - Kill all connections from userspace when client disconnect

I'm too young to die

- Modification of connection tracking entry
  - Change parameters
  - Change timeout
- Set duration of connection
  - Set timeout to a fixed value
  - Expiration at wanted time
- NuFW provides strict time-based filtering:
  - Ex: Strict 8h-18h period with connection destruction at 18h

What's up doc ?

- Integrate with Netfilter tools
  - NuFW handle all conntrack events
  - This is not KISS
  - Informations missing
  - Should use dedicated tools
- Usage of Ulogd2
  - New Netfilter logging software

Something in the way

- Ulogd2 is a rewrite of ulogd:
  - With equivalent capabilities
  - Use new libnf* library
  - More configurable
- Connection logging:
  - Log connections into database by listening on event
  - Advanced SQL storage
- Beta2 should be released this week

Je sens que je vais conclure

- NuFW takes advantage of Netfilter to
  - Provide secure indentity-based filtering
  - Extensive logging
  - Quality of Service
  - Single Sign On
- Netfilter provides impressive tools:
  - Just do it

Questions ?

- NuFW: http://www.nufw.org/
- INL: http://www.inl.fr/
- Software INL: http://sofware.inl.fr/
- Netfilter: http://www.netfilter.org/
- Ulogd2 : http://netfilter.org/projects/ulogd/
- NFWS 2008: http://workshop.netfilter.org/2008
  - Users day, 29 september 2008
- Contact me: eric@inl.fr