

# Netfilter



# A Short History

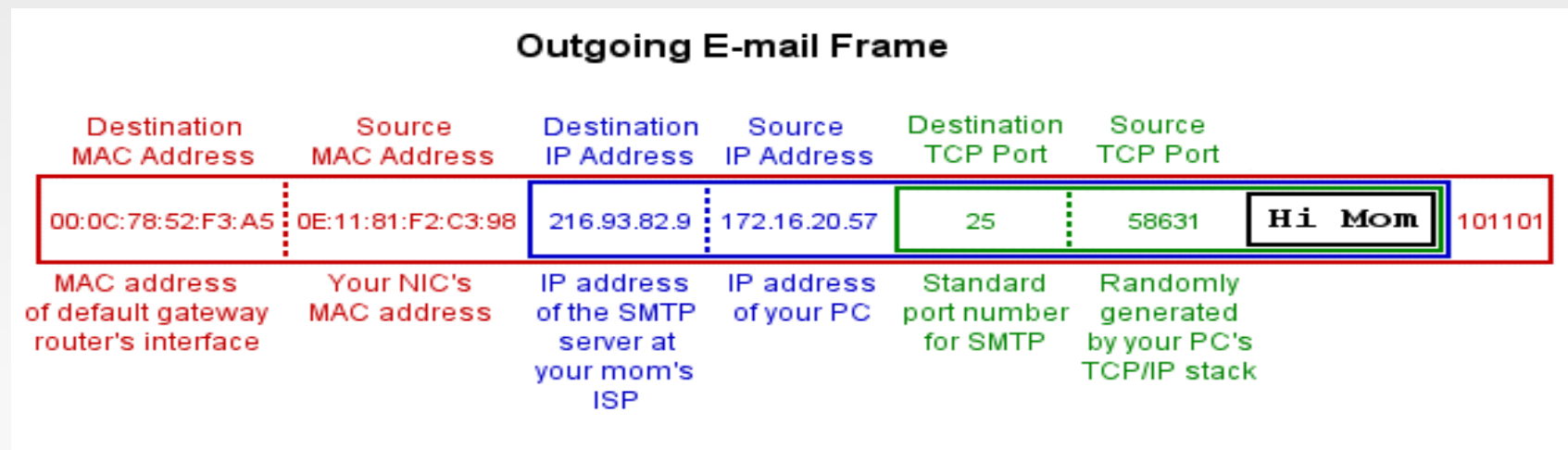
- Rusty Russel
- Ipfawdm (based on IPFW from BSD)
- Ipchains (Linux 2.0)
- Iptables (Linux 2.4)
- Netfilter (current)
- Nftables (Future)
- Maintained by Patrick McHardy
- Netfilter is the first **modular connection aware** firewall for linux
- Netfilter is among the most abused GPL projects

# GUI is BAD, ok

- GUI hides code
- Most projects do not keep up with kernel releases
- Some projects even get fundamentals wrong, such as packet direction
- There are some good options, such as UFW or perl wrap scripts, such as Dynamic Firewall (Daniel Robbins)

# Packets and Frames

- Firewalls operate at OSI layer 3
- Firewalls also provide functions to control layer 2 (MAC)



# Netfilter Basics

- Iptables <chain> <source> <interface>  
<destination> <protocol> <operand> <target>
- Remember kids: There is no implicit deny, unless you write one
- You can use variables to describe netfilter functions: \$IPT=iptables, \$INT=eth0, etc.

# Target Options

- `iptables <chain> <source> <interface> <destination> <protocol> <operand> <target>`
- **Accept** → No more matching
- **Drop/Reject** → Packet dropped
- **Log** → Log entry
- **DNAT/SNAT** → Destination/Source NAT
- **Masquerade** → NAT, Assumes firewall host

# Matching Options

- iptables <chain> <source> <interface> <destination> <protocol> <operand> <target>
- -j → Jump to <target>
- -A → Append to chain
- -F → Delete Table
- -s, -d → source/destination address
- -p → protocol type (tcp, udp)
- -i, -o → input/output interface name
- -t → jump to table

# Connection Matching

- The `-m` option is the most flexible, most powerful tool in netfilter
- `-m -state <state>` tracks whether a connection is previously created, related, new, or invalid

# Connection Tracking

- Tracks connection *state*, relative to current operation
- -m `conntrack -ctstate` → Invalid, Established, Related, New

# Other Netfilter Extensions

- Fuzzy matching
- Rate and connection limiting
- Multiport matching (leelu dallas multipass!)
- Operate every X number of packets
- Operations on packet size
- Tarpit
- Load Balancing

# Designing Firewalls

- Keep in mind what you are intending this firewall to do
- Keep in mind, that if a packet does not match any rules, CHAIN policy applies (no implicit deny)
- Making DROP the default policy is always the smart option
- *REMEMBER:* Rules are matched in the order they are created. Don't nuke port 22, then try to pass packets through it.

# Thanks for Coming!

