IPv6 firewalling

TF-NG Meeting,

Athens (Greece), 15/10/2001

János Mohácsi <Janos.Mohacsi@dante.org.uk>, Network Engineer
DANTE

Contents

- Requirements
- Firewalls and addresses
- IPv6 firewall architecture
- IPv6 firewalls
- Applications
- On going work

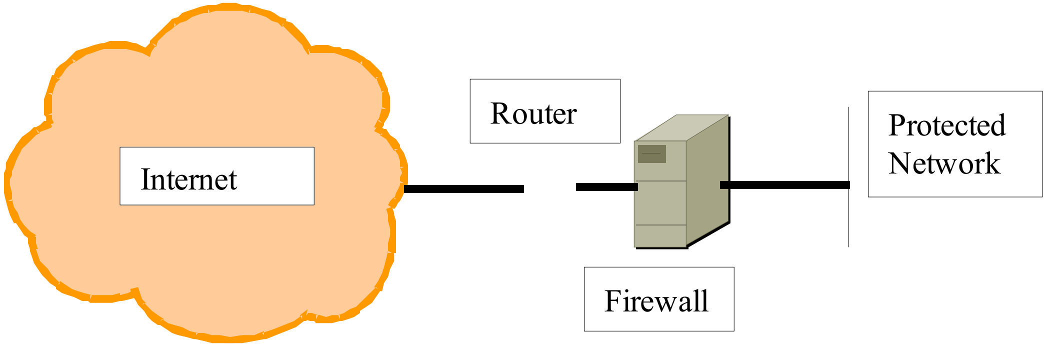
IPv6 Firewalling

- Next generation Internet:
  - Security should be better than currently
- IPv6 architecture and firewall
  - No need to NAT
  - Network scanning virtually not possible (/64)
    - Deny DNS zone transfer
  - Other possible network hiding: DNS splitting
  - Weaknesses of the packet filtering cannot be make hidden by NAT

IPv6 firewalls and addresses

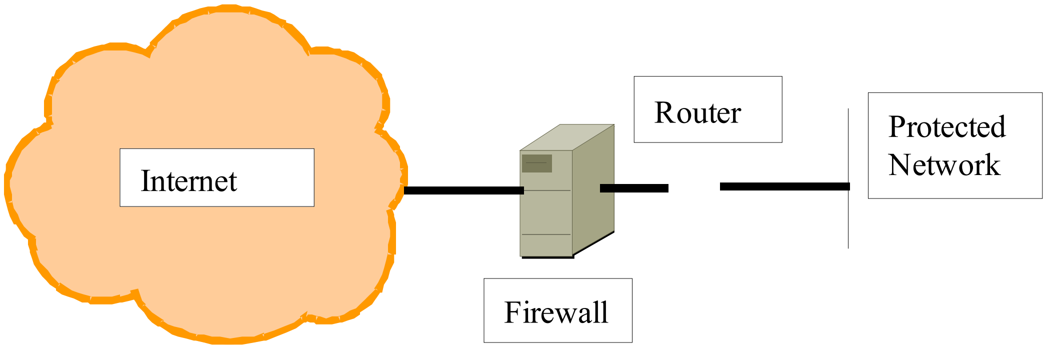
- Current practice of address usage:
  - – global addresses
  - – link local addresses
  - – NO site local addresses - semantics/usage under study at IETF
- Proposal:
  - – allow for local address - (supposing routers are operating correctly)
  - – filter according to the security policy for global addresses
  - – Do not filter ICMPv6! – Neighbor Discovery + PATH MTU discovery

IPv6 firewall usage/1



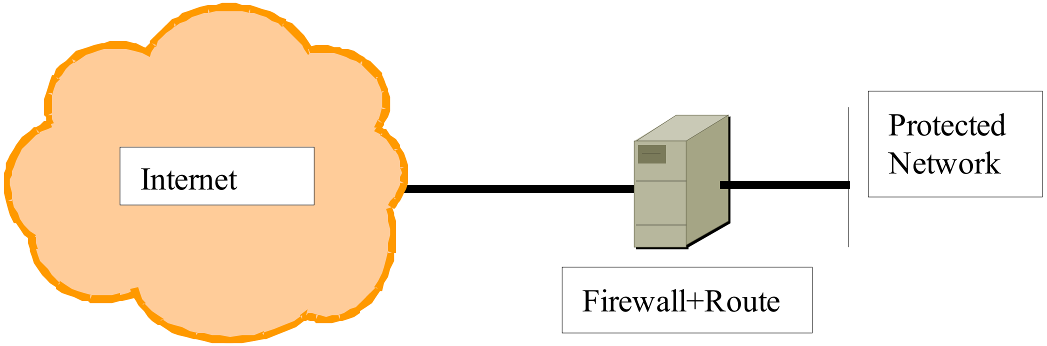
- Internet-router-firewall-net architecture
  - if firewall is prepared for distinguishing IPv6 headers - usable
  - if not prepared - very difficult or not effective filtering

IPv6 firewall usage/2



- Internet-firewall-router-net architecture
  - firewalls are cannot really handle routing protocol correctly - not recommended, unless ?

IPv6 firewall usage/3



- Internet-firewall/router(edge device)-net architecture
  - can be powerful - currently best solution - one point for routing and security policy

Evaluation of IPv6 firewalls: IPfilter

- clean architecture, powerful filtering, quite portable
  - – problems:
    - no IPv6 extension header support; no ftp proxy support; ICMPv6 support is rudimentary (no support for IPv6 defined error conditions); *BSDs contain it, but not compiled with IPv6 support by default
  - – good things:
    - quite complete architecture; well documented, performance degradation negligible

Evaluation of IPv6 firewalls: IP6fw

- clean architecture, good filtering, medium portability
  - problems:
    - architecture not too modern, no proxy support at all, autoconfiguration is not well supported, UDP/ICMPv6 is weakly supported
  - good:
    - IPv6 extension header (not extensive), *BSD contain them with predefined filtering rules

Evaluation of IPv6 firewalls: Netfilter

- complex architecture, good filtering, weak portability
  - problems:
    - development version, proxy only via extra kernel programming, very weak ICMPv6 support, not included in any commercial Linux, poorly documented
  - good:
    - extensive development, correctness test under way, good extensible architecture

Evaluation of IPv6 firewalls: Cisco access list

- simple architecture, weak filtering (basic access control) only, Cisco only
  - – problems:
    - only address filtering
  - – good:
    - commercially supported

Evaluation of IPv6 firewalls: Others

- 6wind:
  - press release - probably worth testing
- ip6fwtk:
  - under test

- Conslusion:
  - Only packet filters:

Interoperability of filtered applications

- FTP:
  - Very complex: PORT, LPRT, EPRT, PSV, LPSV, EPSV
  - virtually no support in IPv6 firewalls
  - HTTP seems to be the next generation file transfer protocol with DAV and DELTA
- Other non trivially proxy-able protocol:
  - no support

Conclusion + Future

- IPv6 firewalls are existing
- They are far from mature
- They can be used for simple firewalling
- Commercial support ?
- Transition problems – on going work
- Mobile IPv6 – other more serious problems…