Mobile IPv6 issues in the presence of Firewalls

Franck Le

draft-le-mip6-firewalls-00.txt

IETF59

NOKIA

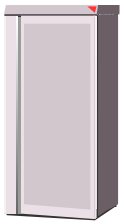
Should MIP6 be worried about firewalls?

- Firewalls are an integral part of most IP networks deployed today
- In most cases, current firewall technologies are unaware of MIPv6
- Firewalls that are MIPv6 unaware will cause deployment problems
- Key issues that firewalls raise (for MIPv6) are captured in the I-D

Stateful inspection packet filters

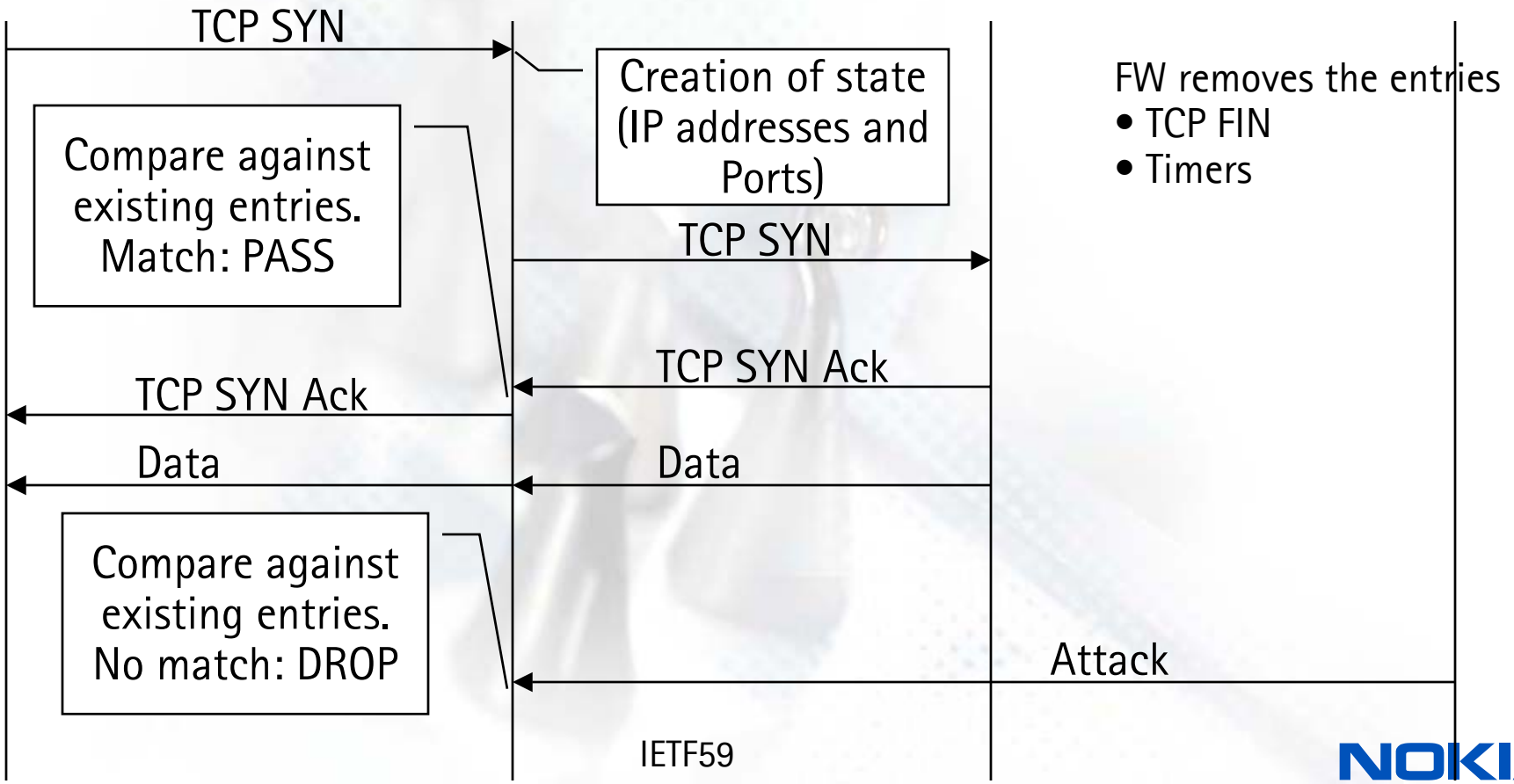
Node protected by firewall

Firewall



Server

Malicious Node

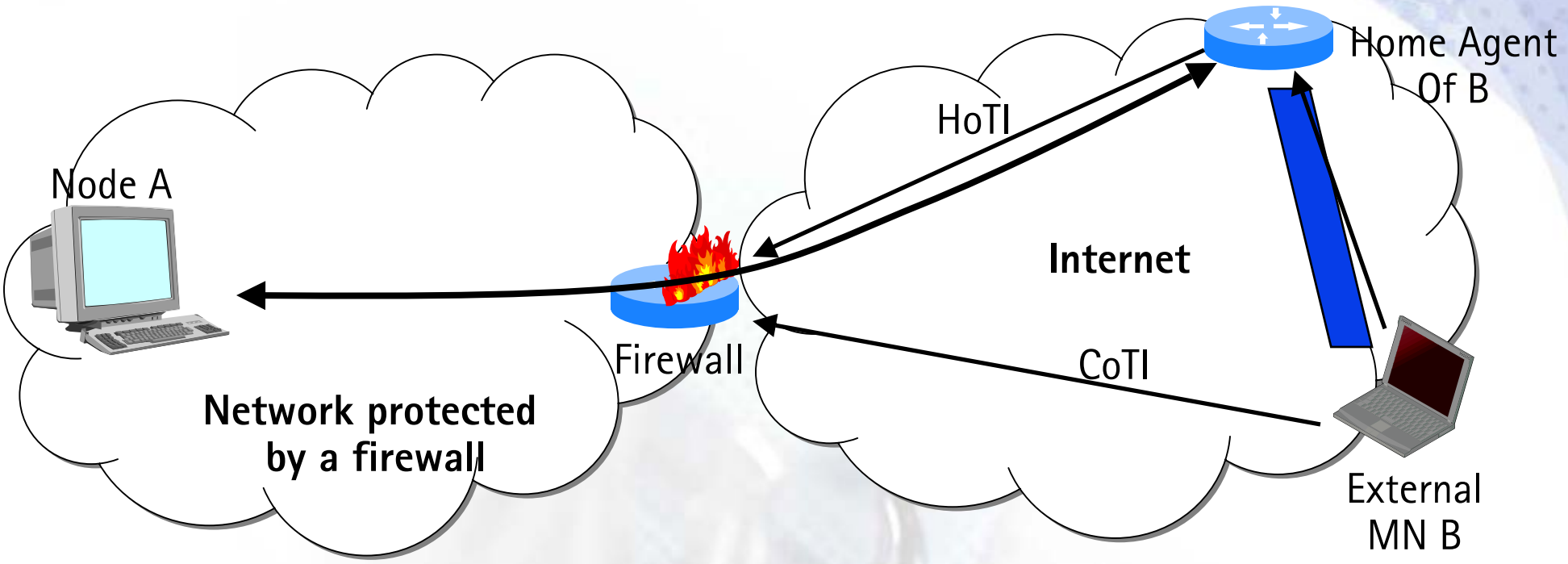


FW removes the entries

- TCP FIN
- Timers

NOKIA

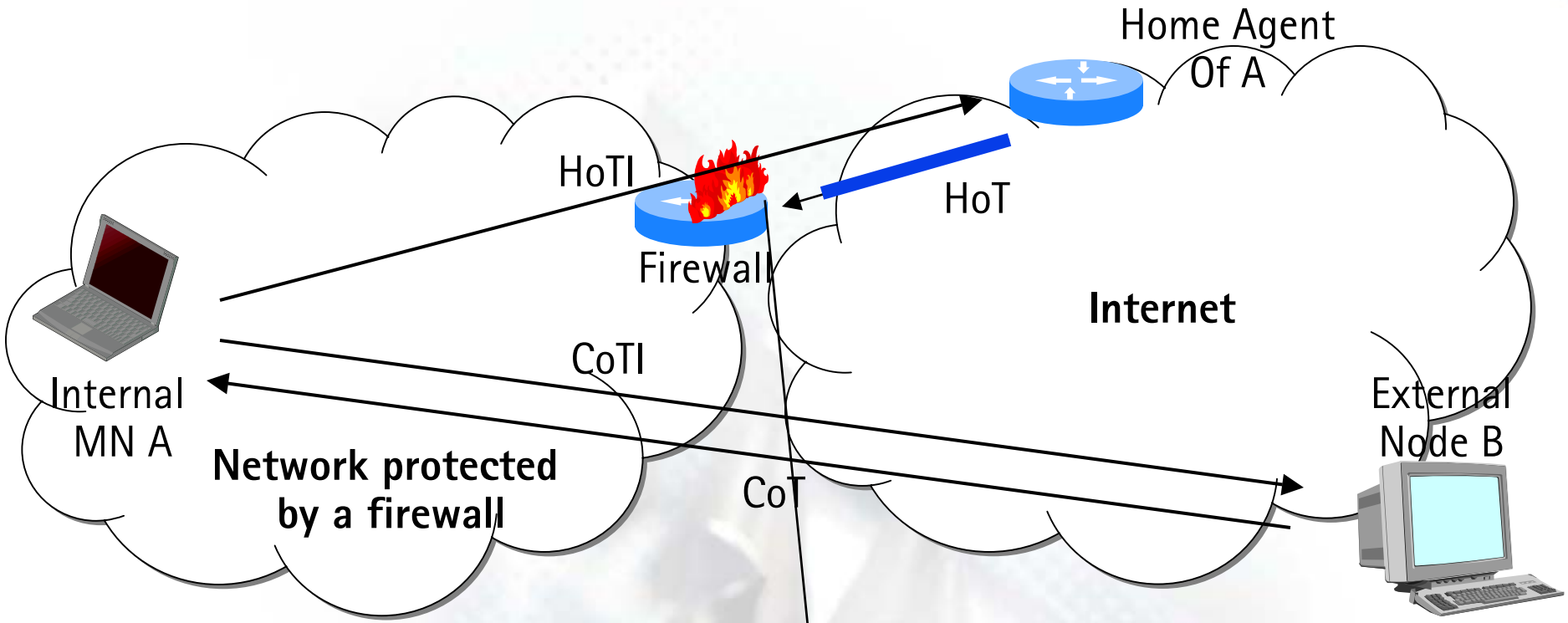
Issue 1 with Return Routability test



- Let's assume a communication between nodes A and B
  - Reverse tunneling
  - Firewall state created: IP A, HoA IP B, e.g. TCP
- MN B may decide to execute the RRT to take advantage of RO
  - HoTI may be dropped (different protocol ID)
  - CoTI may be dropped (different source IP address)

NOKIA

Issue 2 with Return Routability Test



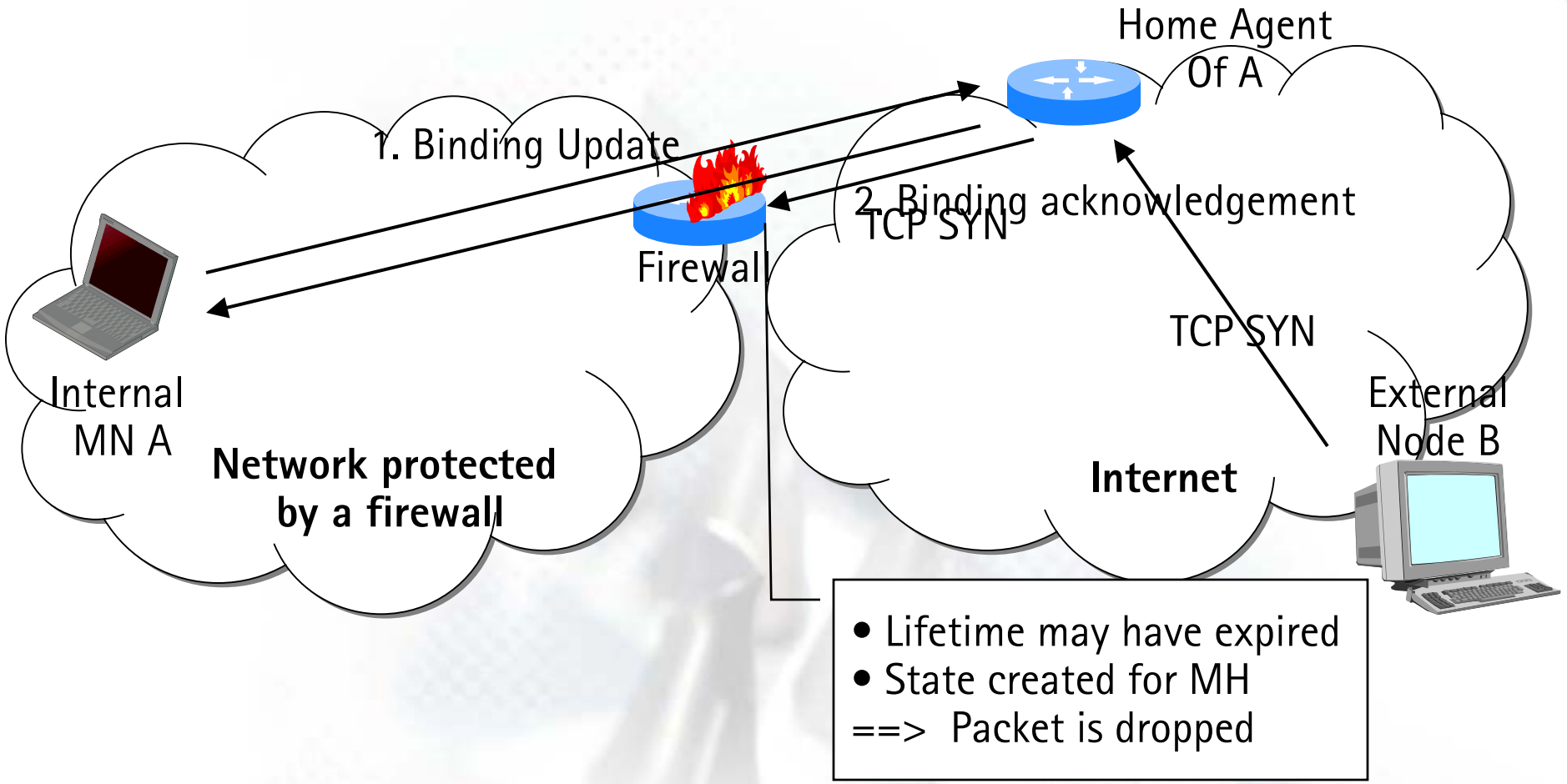
- MIPv6 requires HoT to be ESP encrypted
- Typical FWs however drop ESP packets since they cannot inspect them
- HoT packet may therefore be dropped

NOKIA

Issue with firewall status update

- Let's assume
  - Alternative mechanisms to authenticate the binding update messages are developed
  - Or other mechanisms to let the RRT packets pass through the firewall are developed
- The firewall may still drop the packets coming from the new CoA since these incoming packets do not match any existing entry
- Need to update the states in the firewall as well

Issue - Reachability



NOKIA

Question before WG

- Does the WG think that firewall issues present an impediment to MIPv6 deployment?
- Should firewall issues w.r.t MIPv6 be documented in an informational RFC by this WG?
- Further input to I-D solicited.