Tunnel Establishment Protocol

Pat Calhoun

Charles E. Perkins

pcalhoun@usr.com

cperkins@eng.sun.com

http://www.srvloc.org/~charliep

Tunnel Establishment Protocol (TEP)

Intended to serve a variety of tunnel establishment needs in a consistent way

- multiprotocol tunneling
- multilevel security domains
- virtual private networks

This is a demanding set of requirements

TEP source material

TEP has been synthesized from several existing and outdated drafts

- Virtual Private Networking
- Integrated Mobility Extension
- Tunnel Setup Protocol
- Hierarchical Foreign Agents
- RFC 2002

The process of integration is still ongoing.

Agent Advertisement is not part of TEP, but would be exactly like previous Hierarchical Foreign Agents draft for IP-aware requesting nodes. Alternatively, could try to define solicitations non-IP nodes, or advertisements for them, but this leads too far afield.

TEP is specified to operate using extensions to Mobile IP registration messages, sent to the same port number.

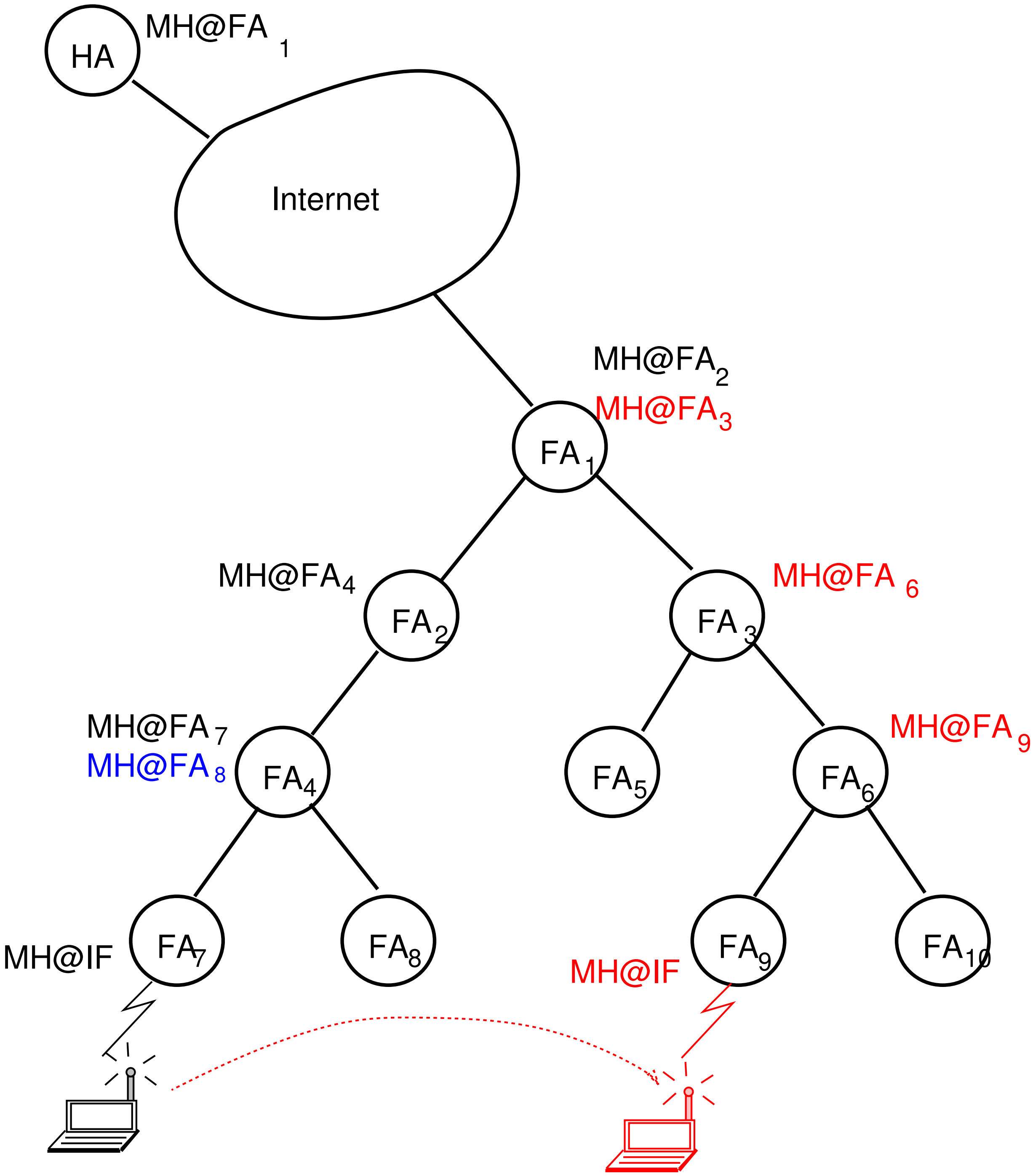
TEP terminology

- targeted tunnel agent (like a home agent)
- foreign agent (was, "requesting tunnel agent")
- mobile node (was, "PDU receiver")

TEP is designed to allowing a multiprotocol tunnel agent (a "foreign agent") request a tunnel on behalf of some node that does not necessarily participate in the protocol (a "mobile node")

TEP is constructed so that the established tunnel is bidirectional.

Hierarchical agents



Previous idea: make Registration Requests go only as far as needed up a hierarchy of Foreign Agents

- Security needs careful attention
  - Establish session key, as outlined in Route Optimization
- Each requesting tunnel agent considers the PDU receiver to be registered at tunnel agent just below it in the hierarchy
- Tunnel Requests passed from level to level
- Likewise for Tunnel Replies

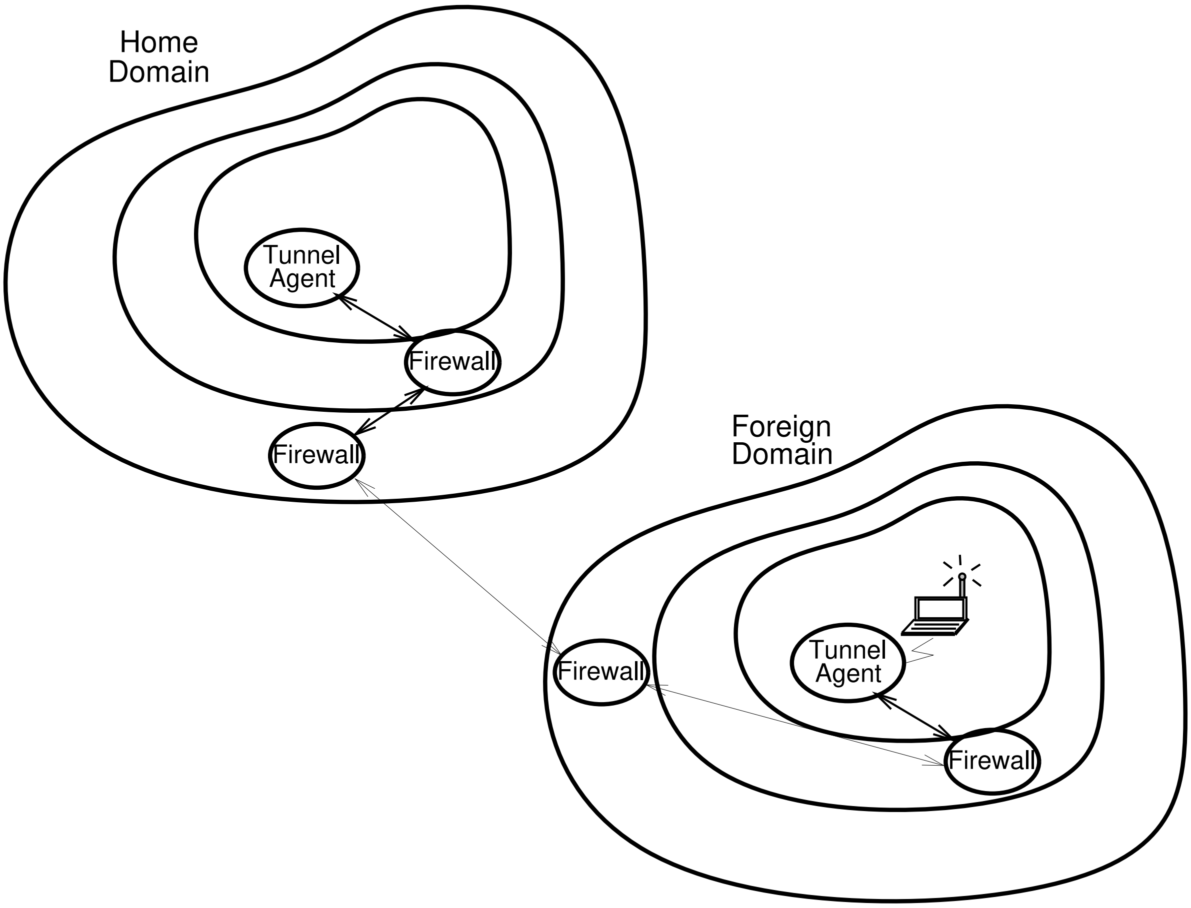
Transitivity of Trust

Agents in two domains have to have a point of trusted contact. TEP is constructed to allow the requesting tunnel agent utilize a trust relationship between a PDU receiver and a targeted tunnel agent.

In addition, trust relationships at other levels of the hierarchy can be used.

TODO: enable association of tunnel parameters at each tunnel stage (may require iterated encapsulation)

Tunneling between two domains



The PDU receiver in the foreign domain should know (by advertisement or preconfiguration) the agent hierarchy in its home domain.

Firewalls have to be tunnel agents, or effectively managed by tunnel agents.