Using IPsec to Secure IPv6-over-IPv4 Tunnels

R. Graveman, M. Parthasarathy,
P. Savola, H. Tschofenig

<draft-tschofenig-v6ops-secure-tunnels-01.txt>

Track: Informational

Using IPsec to Secure IPv6-over-IPv4 Tunnels

- Rationale
  - Tunneling is one transition mechanism
  - IPsec offers a tunneling method with certain properties
    - IPv6 “inside” and IPv4 “outside” is explicitly allowed
    - Cryptographic protection “through the tunnel”
    - Policy enforcement and authentication at endpoints
    - Many issues already addressed:
      - EAP, NAT traversal, ECN, DHCP (Mode_CFG)
  - “Use IPsec” requires additional explanation
    - draft-bellovin-useipsec-03
  - ESP (protocol 50) REQUIRED in IPv6
    - MUST be implemented in dual-stack systems
    - ESP can run in transport mode or tunnel mode
  - IKE(v2) can set up security associations (SAs)

Using IPsec to Secure IPv6-over-IPv4 Tunnels

- Approach uses:
  - draft-ietf-ipsec-rfc2401bis-02
    - Security Architecture for the Internet Protocol
  - draft-ietf-ipsec-esp-v3-08
    - IP Encapsulating Security Payload (ESP)
  - draft-ietf-ipsec-ikev2-14
    - Internet Key Exchange (IKEv2) Protocol
  - draft-ietf-ipsec-ikev2-algorithms-05
    - Cryptographic Algorithms for use in the Internet Key Exchange Version 2
  - draft-ietf-ipsec-udp-encaps-09
    - UDP Encapsulation of IPsec Packets
  - Tunnel Mode: site-to-router, host-to-router, host-to-host
  - Transport Mode: router-to-router

Open Issues

- Add text on using IKEv1
- Discuss “Use of IPsec Transport Mode for Dynamic Routing,” draft-touch-ipsec-vpn-07
- Add more detailed description of the address configuration mechanism
- The configuration example with CFG_REQUEST/ CFG_REPLY payloads should contain IPv6 addresses.
- Add the full-fledged example of Section 10
- Add notes on the implications of mobility interworking
- Discuss the use of link-local etc. with Tunnel mode SAs
  - How many SAs will be needed (and how they are negotiated) if link-local messages will be present as well?
- Strengthen Site-to-Router scenarios–better ideas on how to categorize these?
- Improve discussion of transport versus tunnel mode SAs

Next Steps

- Comments?
- Post -02 draft?
- WG document?

Specific Comments

- Transport mode seems equal to tunnel mode in security (especially in site-to-router/router-to-site cases) if you just use strict RPF -like ingress filtering at the ISP's side.
- Transport mode is obviously weak when you don't do ingress filtering compared to tunnel mode (i.e., in my mind the main difference of tunnel/transport mode is that with tunnel mode, strict ingress filtering is a built-in feature!)
- Transport mode requires IPsec-bis, hence IKEv2, if there aren't implementations already supporting mixed-mode transport mode.
- Tunnel mode may have complexities regarding link-local etc. messaging.
- The terminology about host-to-host, router-to-router, etc. should be reconsidered, considering the most interesting issue in endsite-to-router/router-to-endsite is roughly equal whether it's a host or router that attaches to the ISP -- one uses a prefix, the other an address (or a /64 prefix).