Simple Security in IPv6
Residential Gateway CPE
draft-ietf-v6ops-cpe-simple-security
Motivation

- RFC 4864, Local Network Protection for IPv6, recommends simple security for residential gateways.
- Does not go into much detail.
- Just says, basically, outbound flows to be generally allowed and inbound flows to be generally refused.
- Applications developers to benefit if vendors of residential CPE have more detailed recommendations.
Scenario Overview

- Routing for home and very small office use.
- May be deployed by users with no significant expertise in internetworking.
- May be integrated with IPv4/NAT functions that users are familiar with today.
- IPv6 simple security intended to be functionally similar to IPv4/NAT simple security.
Similarities with IPv4/NAT

- Filtering behaviors for TCP, UDP, and ICMP as recommended by BEHAVE for IPv4/NAT.
- Transparency helpers may be required for some application protocols, e.g. FTP, RTSP, SIP.
- Alternatively, techniques like STUN and TURN.
- Hole-punching for passive listeners, i.e. UPnP IGD or its alternatives.
Special IPv6 Considerations

- Teredo blocked to prevent bypassing simple security.
- IPsec AH, ESP and IKE allowed.
- IP-in-IP and GREv1 allowed.
Recent Updates

- Recommendations for SCTP and DCCP filtering.
- Removed some recommendations regarding Teredo.
- Added a lot of normative and informative references.
- Many editorial changes.
Open Issues

- The passive-listener clusterfumble.
- Are there any other remaining troubles?
The IETF Protocol Stack

Religious
Political
Financial
Application
Presentation
Session
Transport
Network
Datalink
Physical

You are here.