Balanced Security for IPv6 CPE

draft-ietf-v6ops-balanced-ipv6-security-00

IETF88 Vancouver

M. Gysi, G. Leclanche, E. Vyncke, R. Anfinsen

Status

- Personal draft -00 posted on 25 January 2013
- -01 posted on 29 July 2013
- Accepted in Berlin (IETF-87) as WG document

Problem Statement Which security policy for IPv6?

- RFC 6092: Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
  - either blocking all inbound or allowing all inbound connections
  - Implementations exist in low-end CPE
- draft-vyncke-advanced-ipv6-security-03
  - Use more advanced filtering techniques such as IPS, reputation database, ...
  - More a Universal Threat Mitigation for large SMB/organization
  - No implementation exists in low-end CPE

Balanced Security ?

Security
End-to-End Connectivity

Balanced Security?

- Based on Martin & Guillaume's idea for their Swisscom IPv6 CPE
  - Switzerland has 10% of IPv6-penetration dixit Google
  - Deployed for several months now in CH
  - Ragnar will do the same in NO
- Works like RFC 6092 in open mode
  - Allow all inbound traffic
  - **EXCEPT for well-known exceptions**

Changes in -00

- Presented by Ragnar at RIPE and got a lot of positive feedbacks
- Basically, watered down, no more ‘suggestion’ and now a lot of ‘FOR EXAMPLE’ in order to avoid IETF being liable for any permit/deny port list suggestion
- List of ‘dangerous’ port is based on poor protocol spec or poor implementation
- Added remote management over IP (in case of non TR-69 CPE)
- Mentionned that stateless / stateful filtering is irrelevant in this I-D (of course one is more ‘secure’ than the other)

- Thanks to all reviewers

Next Steps?

- Baring comments and discussion on the example of ports, should we go WG last call?