# Balanced Security for IPv6 CPE

draft-ietf-v6ops-balanced-ipv6-security-01

IETF89 London

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
- -00 posted on 21 October 2013
- Sent to WGLC in Vancouver (IETF-88)
- -01 posted on 5 December 2013

# Changes in -01

- Basically, watered down and English text clean-ups
- It seems that more ISP are doing this open by default except a few ports.
- New X/Box:
  - Uses IPv6 when clear communication between consoles (i.e. no filtering)
  - Else, it falls back to Teredo...

# Watering Down

*As of 2013, Swisscom has implemented the rule ProtectWeakService as described below. This is* ***meant as an example and must not be followed blindly****: each implementer has specific needs and requirements. Furthermore, the example below will not be updated as time passes, whereas threats will evolve.*

# Added Flexibility

*This pre-defined policy should be centrally updated, as threats are changing over time.  It could also be a member of* ***a list of pre-defined security policies*** *available to an end-customer, for example together with "simple security" from [RFC6092] and a "strict security" policy denying access to all unexpected input packets.*

# Last Word of Caution

*Depending on the extensivity of the filters**, certain vulnerabilities could be protected or not.** It does not preclude the need for end-devices to have **proper host-protection** as most of those devices (smartphones, laptops, etc.) would anyway be exposed to completely unfiltered internet at some point of time. The policy addresses the major concerns related to the loss of stateful filtering imposed by IPV4 NAPT when enabling public globally reachable IPv6 in the home.*

# Comments from a Reviewer

- Title change:
  - ~~Balanced Security for IPv6 Residential CPE~~
  - A Security Profile for IPv6 Home Networks CPE
- Adding
  - *“However, the end-user shall be able to change the default setting to the [RFC6092] profile if deemed appropriate.”*
- Remove
  - the ‘Threats’ section
  - *“To the authors' knowledge, there has not been any incident related to this deployment in Swisscom network”*

# Next Steps?

- Is this a useful I-D?
- Should we change the title?
- Should we “neutralized” it even further?
- Authors will implement suggested changes
- After, should we re-do WG last call?