Balanced Security for IPv6 CPE

draft-v6ops-vyncke-balanced-ipv6-security

IETF87 Berlin

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

Status

- -00 posted on 25 January 2013
- -01 posted on 29 July 2013
- Some comments on the list (see later)

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 ?

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**

Exception?

- Some applications (identified by ports) are blocked:
  - Either inbound
  - or inbound_and_outbound
- Apps assumed to be too dangerous if exploited from outside
  - SSH, Telnet (!), HTTP (but not HTTPS), remote desktop
- Apps that should not cross the SP CPE ‘boundary’
  - RPC, NetBIOS, 445/TCP, AFP, ...

Changes in -01

- Also applicable to mobile ISP (then implemented at GGSN)
- ‘fixed policy’ -> ‘pre-defined’ policy which subscribers can change
- CPE/MSSP GUI should also allow change to both RFC 6092 policies (open/close)

- Thanks to Simon Leinen, Eduard Metz

Next Steps?

- Not sure about becoming WG item but we feel that this was useful to document
  - Informational RFC?
  - Suggested to move it to OPSEC or OPSAWG ?
  - And fixed the filename of the I-D of course ☹