Balancing End-user Security and End-to-end Connectivity

Ragnar Anfinsen
CPE and IPv6 Architect

The Question

- IPv6 CPE Firewall – Default ON or OFF?

- Quite strong feedback from the community and mailing-lists;
- Firewall off:
  - We finally can get back full end to end connectivity
  - Makes no sense to have a firewall; IPv6 enabled OS's are secure enough
  - Operators doing FW off; No problem.
  - FW does not add to security. Spam and botnets are the biggest problem.

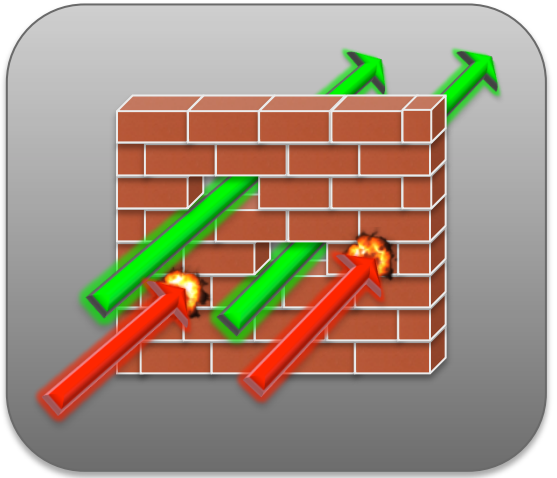
- Firewall on:
  - Customers are used to the NAPT "security", do not mess with that.
  - Marketing is afraid of the implications by not having a security layer.

How do we do IPv6 security today?

- RFC 6092: Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
  - Either block all inbound connections or allow all outbound connections
  - Implementations exist in low-end CPE

How do we do IPv6 security today?

- Block all inbound and allow all outbound
- The customer can edit the port forwarding rules
- But still all non-open ports are blocked
- Not very good for end-to-end connectivity
- Xbox One reverts to IPv4 if IPv6 firewall is present



IPv4 NAT ≠ IPv6 Firewall

- IPv4 NAT: (Generally) allows TCP hole punching. E2E TCP communication is possible with the help of a "rendezvous server", as NATs generally use endpoint independent mapping
- IPv6 Firewall: (Generally) does not allow TCP hole punching (if it is implemented using Linux iptables, which uses address and port dependent filtering). Will severely impact the user's experience.

The solution?

Balanced Security for IPv6 Residential CPE

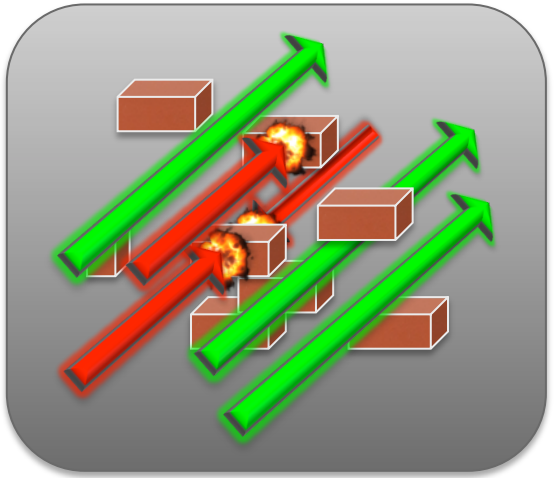
draft-ietf-v6ops-balanced-ipv6-security

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

http://tools.ietf.org/html/draft-ietf-v6ops-balanced-ipv6-security-01

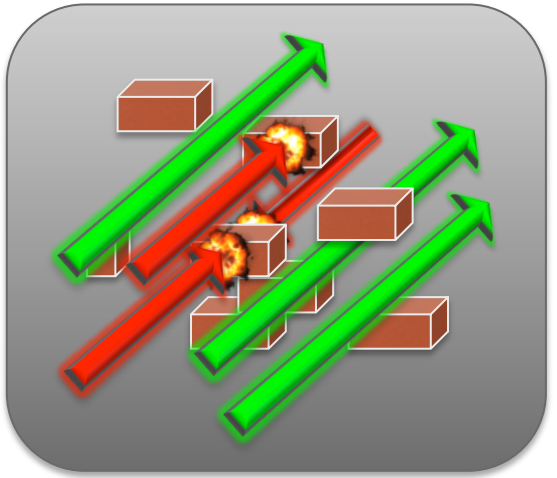
Balanced Security

- Works like RFC 6092 in open mode
  - Allow all inbound traffic
  - **EXCEPT for defined exceptions**



Typical Exceptions

- 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, NTP
- Apps that should not cross the SP CPE ‘boundary’
  - RPC, NetBIOS, 445/TCP, AFP, ...



Managing Exceptions

Several options:

- BCOP Document defining a default exceptions list, community effort
- SP could define their own default exceptions list

- List in draft only provided as an example. Shows Swisscom list at the time of writing the draft.

Deployed?

- Swisscom has implemented and deployed this
- No operational difficulties reported
- No incidents reported

- Altibox will implement this soon

Do the operators find this useful?

Does a BCOP document defining the exceptions make sense?

What do you do on your CPE's?

Want to contribute?

Please see me during the meeting, or contact me or the authors on email:

Eric Vyncke: evyncke@cisco.com
Martin Gusi: martin.gysi@swisscom.com
Guillaume Leclanche: guillaume.leclanche@viagenie.ca
Ragnar Anfinsen: ragnar.anfinsen@altibox.no

Questions?
Comments?