On Firewalls in Internet Security
draft-ietf-opsawg-firewalls

Fred Baker, Cisco
Paul Hoffman, Cybersecurity Association
Since our last meeting...

- We got lots of great comments, but no particular direction or feeling of consensus.
- It is not at all clear what “best current practice” or “best advice” would be for operators would be given the wide variety in feature sets and quality of firewalls.
- So, we propose a major change in focus of the document (and probably a new title).
Start with the abstract

Current:
This document discusses the most important operational and security implications of using modern firewalls in networks. It makes recommendations for operators of firewalls, as well as for firewall vendors.

Proposed:
Remove the second sentence: no more recommendations
We can probably agree on the operational implications

- For example, “A firewall that blocks traffic of type X that is put at the edge of an administrative boundary will have this operational effect”
- Or “A firewall that changes packets of type Y that is put inside an enterprise (not at an edge) will have this operational effect”
Modern firewalls

- Filter on more variables than what we might want
- Route, but often not as flexibly as devices we call “routers”
- Tunnel some traffic between two places (such as through IPsec VPNs)
- Can act as NATs, of various quality
- Maybe we can catalog this succinctly
Firewalls appear in many places in an enterprise

- The edge is common
- Internal is now becoming common, particularly for segmenting by department and for compliance in some environments
- Host-based firewalls, often not administered centrally
- The position changes the operational effect
Goals for the proposed new document

- Be informative for network operators (and not necessarily anyone else)
- Tell operators things about modern firewalls they maybe didn’t know
- Be informative, not prescriptive
- Finish in a year
- Have broad WG consensus
Content of the proposed new document

• Use shorter declarative sentences
• Difficult topics are called out but then are not belabored
• Name and describe both standards and proprietary technologies
• Keep the focus on operators, not security folks
This is a WG document

- Does this proposal work for you?