On Firewalls in Network Security

(draft-gont-opsawg-firewalls-analysis)

Fernando Gont
Fred Baker

IETF 95
Buenos Aires, Argentina. April 3-8, 2016

Goals of this document

- Recognize role of FWs in internet architecture
- Analyze common kinds of FW and associated claims
- Analyze assumptions made around firewalls
- Analyze trade-offs in different paradigms
- Provide conceptual guidance wrt use and deployment of FWs
- Identify harmful behavior and provide advice
- Trigger other work in this area

But...what do we mean by “firewall”?

- A device or software that imposes a policy whose effect is "a stated type of network traffic may or may not be allowed from A to B".
- May reside in the host or the network
- May be implemented in general-purpose system or in special-purpose middle-ware device.
- May operate at different layers
- The layer at which the firewall operates has implications on the types of policies it may apply

Role of Firewalls in Network Security

- Firewalls provide prophylactic perimeter security
  - analogous to the service provided by the human skin to the human body
- Firewalls do not prevent the need for the stronger solutions
  - they rather make their expensive invocation less needful and more focused.

Firewalls and the E2E Principle

- One common complaint about firewalls is that they violate the E2E Principle.
- However, the E2E Principle:
  - is a plea for simplicity
  - argues against behavior that from the pov of a higher layer introduces inconsistency, complexity, or coupling
  - does **not** forbid e.g. lower layer retransmissions, nor maintenance of state, nor consistent policies imposed for security reasons

Common Kinds of Firewalls

- **Context or Zone-based firewalls**
  - protect systems within a perimeter from systems outside it
- **Pervasive routing-based measures**
  - protect intermingled systems from each other by enforcing role-based policies
- **IPS systems**
  - analyze application behavior and trigger on events that are unusual, match a signature, or involve an untrusted peer

Firewalling Strategies

- **Default-deny**
  - traffic is blocked unless it is explicitly allowed
  - Fails on the “safe side”
  - Prevents deployment of new features and applications
- **Default allow**
  - traffic is allowed unless explicitly blocked
  - typically enforced at perimeters where a comprehensive security policy

Assumptions on addresses & ports

- IP addresses and transport protocol ports are typically assumed to be stable
- IP address stability
  - Assumption changes with IPv6 temporary addresses (RFC4941)
- Transport protocol port numbers
  - More of a short-cut than a design principle
  - Think about DNS SRV records or Portmap
  - Also consider apps such as FTP and SIP

Assumptions on addresses & ports

- Tendency to multiplex apps on usually-allowed ports
  - e.g., tunnel apps on port 80

State Associated with Filtering

- **Stateless filtering**
  - Decision solely based on the incoming packet
  - Scales well
- **Stateful filtering**
  - Decision based on incoming packet and existing (or lack of thereof) state
  - Allows for more powerful filtering
  - Does not scale well
  - Filtering device can become target of DoS attack

Areas where FWs could do better

- **Enforcing Protocol Syntax at the FW**
  - Some FWs check that e.g. reserved bits are set to 0
  - This prevents incremental deployment on new features and protocol extensions -- e.g., TCP ECN, DNSec

Moving Forward

- Adopt as an opsec WG document?