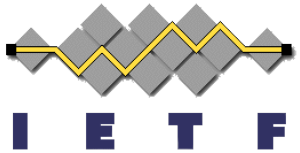
On Firewalls

Fred Baker and Paul Hoffman

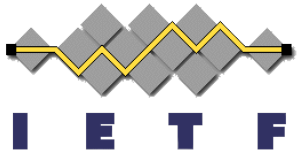
draft-ietf-opsawg-firewalls-01.txt



History

- Fred discussed draft-ietf-opsawg-firewalls-00.txt at IETF 83
  - Working group interest
  - Some mailing list comments
- Paul offered to co-author, and wanted to reorganize
  - Around IETF 84, we were each waiting for the other to do something. oops
- Current state:
  - -01 is a reorganized outline with some text
  - Looking for working group input, including text

Definition of a firewall

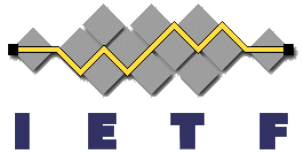


- Turned out to be an important discussion point between authors – very different views
- The definition we agreed on:
  - ***a firewall is … a device or software that imposes a policy whose effect is "a stated type of packets may or may not pass from A to B".***
  - Perimeter defense – but not all perimeters are equal
- Possible interpretations include not only data plane filters but control-plane policies
  - NAT/NAT-like zone filters (the NAT doesn't have a translation)
  - ACL zone filters (the firewall prevents data traffic)
  - Anomaly and signature based IDS (the IDS detects and prevents an attack)
  - Specialized routing behaviors such as null route or reverse path forwarding
  - Selective advertisement of routing information (the sender doesn't have a route to an address such as RFC 1918 or ULA)
  - Role-based systems – one "tenant" can talk to another but not to a third
  - Application-layer gateways
  - …

“Perimeters” imposed

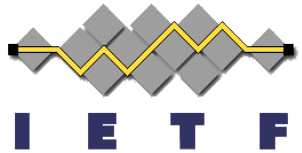
- Layer 3:
  - IPv4 and IPv6 source/destination
- Layer 4:
  - TCP/UDP Ports; need SCTP support, etc.
- Layer 7:
  - ALG/DPI firewalls can filter based on the application protocol contents

Non-firewalls with similar features



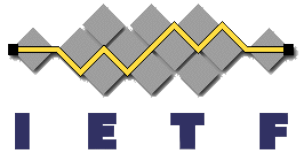
- NAT when it is not used as a security policy
- IPsec or SSL VPN when used to implement trusted connectivity
- Traffic prioritization and TCP performance management

Common complaint: End-to-end Principle



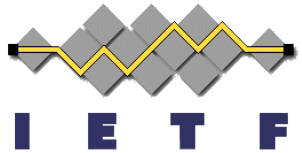
- Claim is made that firewalls violate the end-to-end principle
  - Not accurate
- End-to-end Principle:
  - ***A lower layer entity should not do something that surprises an upper layer entity***
  - "End to End Arguments in System Design", Saltzer, Clark, Reed 1984
- Connectivity policy:
  - A firewall that imposes a consistent policy is not a lot different than a disconnect
  - A network element that operates unpredictably violates the end-to-end principle

What does a firewall defend?



- Second level of defense for hosts and applications
  - “Defense in depth”
  - Makes attacks thread multiple defenses
- Primarily a defense of infrastructure
  - Preserves protected bandwidth and equipment for a business purpose
  - Helps impose a distinction between local and global servers/services

Initial text in place, needs work



- Firewall policies and categories
- Recommendations for operators
- Recommendations for vendors