Impediments to Transport Innovation

On Walls and Gates

Joe Hildebrand (@hildjj)

What firewalls do (TCP)

Photo: Thomas Wolf (CC BY-SA 3.0)

- Allocate state for 5-tuple at session start
  - Session start via SYN/SYN-ACK.
- Checks well-formedness and permission
- Ensures remote IP address can both source and sink traffic
- Allow further traffic in both directions until shutdown
  - Shutdown on FIN/RST, timeout after hours idle, refresh on any traffic, RST after idle
- “Better than 5-tuple” attack resistance by RSTing out-of-window segments

Signals are implicit, based on assumptions about how TCP stacks work.

RST control based on ability to inject unauthenticated traffic into a session.

What firewalls do (UDP)

- Allocate state for 5-tuple at session start
  - Session start via any traffic on unseen 5-tuple
- Checks well-formedness and permission
- ~~Ensures remote IP address can both source and sink traffic~~
- Allow further traffic in both directions until shutdown
  - Timeout after *seconds* idle, refresh on *outbound* traffic, ~~RST after idle~~
- ~~"Better than 5-tuple" attack resistance by RSTing out-of-window segments~~
- Several off-path methods for pinholes (PCP, NAT-PMP, UPnP)
  - Not ubiquitous: too many choices, complexity

Both signaling and control impaired with respect to TCP

Reducing UDP blocking and rate-limiting

Why do network operators and enterprises block and rate-limit UDP?

- Large amounts of attack traffic, prevalence of vulnerable services
  - Widely deployed protocols subject to reflection/amplification attacks
- Firewalls can’t help much: open to off-path DoS, easy to open pinholes
  - Rate-limiting is only current mechanism for protection at scale

But the kinds of transports built on UDP are changing.

- Firewall feature parity with TCP becomes essential for some UDP traffic
- Explicit signaling at a substrate is preferable to continued inference

The goal