Firewall Architecture for

RSVP

Michael Speer

speer@eng.sun.com

Goals

- It should be possible to propagate a flow over the firewall while maintaining the conceptual identify of the flow. This implies:
    - PATH/RESV/TEAR messages from a sender on one side of the firewall should be forwarded/regenerated on the on the other side for the benefit of downstream routers and potential receivers.
    - The data packets that make up the flow should be forwarded/regenerated on the other side of the firewall.
- RSVP messages should on be allowed to cross the firewall when the corresponding data packets that make up a flow are allowed to cross the firewall (and vice versa).

Goals (Continued)

- PATH/RESV/TEAR messages that originated from one of the firewall should be authenticated before being relayed to the other side of the firewall
- RSVP Messages should available for:
  - Firewall local resource management
  - Traffic policing of flows to prevent bandwidth attacks from the outside and traffic disruption from the inside.

Filering Routers

- Router not multicast/RSVP-aware (i.e., encapsulated tunnel through allowed through filter):
    - Allow all packets, or filter on encapsulated header.
    - If filter on encapsulated header, add additional filter criteria for RSVP messages.
    - No RSVP reservations at router. Bandwidth-based denial of service still possible
- Router multicast-aware but not RSVP-aware:
    - Add additional filter criteria for RSVP messages.
    - No RSVP reservations at router. Bandwidth-based denial of service still possible.

Filering Routers

- Router multicast/RSVP-aware:
  - Normal state is to disallow multicast data without filter criteria, but allow RSVP PATH/RESV messages.
  - Authenticated RESV/PATH messages used to instantiate firewall filters in addition to flow reservation filters. PTEAR/RTEAR/Timeouts clear firewall filters in addition to flow reservation state.
  - Can restrict to just one side of firewall, and to just PATH- or RESV-based instantiation.
  - Standard packet scheduling mechanisms apply. Can prevent bandwidth-based denial of service via flow separation.

Issues

- Source Spoofing
- Bandwidth Attacks

Proxy Relay / Bastion Host

- PATH/RESV messages mapped from one side of host to other.
- Apply application-based admission control to determine if proxy can provided requested QoS.
- Only passed if other application-based authentication criteria met.
- Issues:
  - Reply with RESV immediately or only after down-stream host/router responds?
  - Relationship between flow state and session state (e.g., does RTEAR cause termination of proxy)? Initial assertion: should be independent.

Futures

- PATH/RESV/PTEAR/RTEAR Authentication
- Internet Draft by the next RSVP Teleconference.