IETF firewall traversal activities

Melinda Shore

Cisco Systems

mshore@cisco.com

Agenda

- “Firewall” ≈ (Firewall || NAT)
- Background
- Current work
- Future
- Working with IETF
- Coda: Cisco efforts

Firewalls, NATs, ?

- **In IETF, NAT traversal and firewall traversal treated similarly**
  - **Except for BEHAVE, more on that later**
- **NAT and firewall tend to sit at similar places in networks, perform (accidentally) similar functions**
- **Firewall is policy-based mechanism, NAT is not**
- **NAT modifies packets in transit, raises harder architectural questions**

Early work

- SOCKS (product of Authenticated Firewall Traversal working group)
  - Mechanism to allow secure proxying/relaying of individual data streams
  - Doesn't support UDP
  - Doesn't support NAT
  - Moderately wide deployment
- RSIP (product of NAT working group)
  - Mechanism to allow secure proxying/relaying of individual data streams
  - Endpoint uses RSIP to acquire address/port pair from NAT
  - UDP support optional
  - Doesn't support firewall
  - Not deployed much
- RFC 3093 - "Firewall Enhancement Protocol"

Background

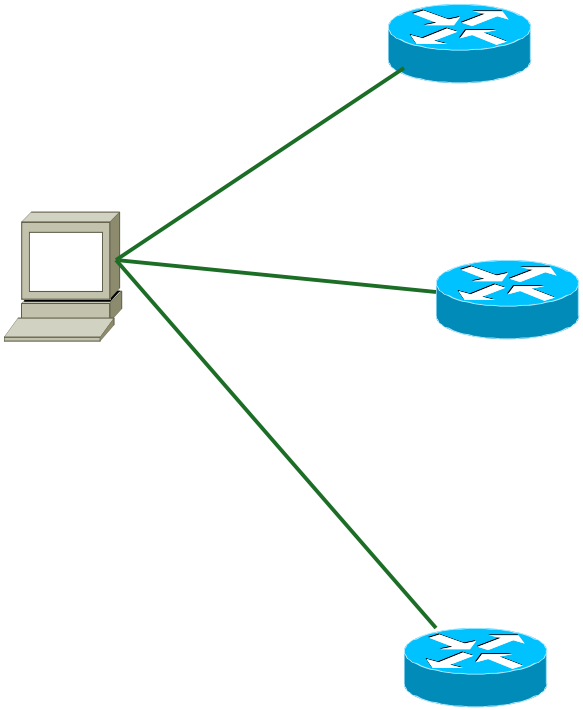
- VoIP uses distinct signaling (control) and media (voice) channels
- Signaling channel usually on well-known port, media channels allocated dynamically at run time
- Call control servers may be used to relay signaling on behalf of NATted endpoints (“trapezoid”)
- Firewalls and NAT traversal problems usually addressed through use of ALGs
- ALGs will not work when signaling is encrypted
- ALGs will not work when signaling and media traverse different firewalls
- VoIP and video media are typically carried over UDP - UDP support is critical

More background

- Around 1999, EP TIPHON brought firewall traversal problem to the IETF, with proposal for firewall control
- About the same time, Jonathan Rosenberg brought similar proposal
- midcom working group chartered as a result of requirements from VoIP community
- off-path vs on-path within the IETF

Off-path firewall control

- **“Off-path”: direct communication between application entity and middlebox**
- **AKA “path-decoupled”**
- **Device location discovered through configuration or discovery**
- **Routing can be very hard**



On-path firewall control

- **Request sent between application peers**
- **Intercepted by middleboxes en route**
- **Solves some hard topology problems**
- **Just about impossible to deploy in real networks**

midcom

- "middlebox communication"
- Intended to generalize beyond firewall/NAT to other types of middleboxes
- Working method:
  - Define requirements
  - Evaluate existing IETF protocols against requirements
  - Choose
- SNMPv3 was chosen as midcom protocol
- *Really* unpopular choice
- Protocol passed WG last call, currently in IESG review
- http://www.ietf.org/html.charters/midcom-charter.html

nsis

- "Next steps in signaling"
- Originally intended to be a next-generation RSVP
- At Cisco we noticed that midcom introduced some very hard topology problems
- Developed RSVP-based firewall/NAT traversal protocol called "Topology-Insensitive Service Traversal"
- Work was turned into an nsis deliverable
- Should be going into WG last call in the next few months
- http://www.ietf.org/html.charters/nsis-charter.html

Newer work

- **SIMCO**
  - **Purpose-developed protocol using same protocol semantics as midcom**
  - **Published as experimental, RFC 4540**
  - **Picked up by Asterisk (open source VoIP PBX) community, released by Digium as midcom library**
- **behave**
  - **Intended to define the behavior of “well-behaved” NATs**
  - **Targeting unmodified NATs**
  - **STUN/TURN/ICE**
  - **Starting to branch out towards carrying policy in STUN requests**

Newest work

- Paul Francis (Cornell University) has proposed IRTF working group based on off-path communication between applications and network devices
- Components of work include
  - Naming
  - Rendezvous
  - off-path service requests
- Originally middlebox work focused on NATs but is now being extended to firewalls
- “offpath” BOF held in Montreal
- relabeled as EMERG (“end-middle-end research group”) to meet in San Diego
- See http://www3.ietf.org/proceedings/06jul/offpath.html
- Won’t produce standards

Sporadic work

- **Distributed firewalls BOF -- motivated by `Ioannidis, S. and Keromytis, A.D., and Bellovin, S.M. and J.M. Smith, "Implementing a Distributed Firewall"`**
  - **2 BOFs held, broad participation, never went anywhere**
- **"Distributed security" BOF (distsec)**
  - **Basically distributed firewalls**
  - **Experience in IETF was similar to distributed firewalls**
  - **Mailing list still alive, but quiet**
  - **https://www.machshav.com/mailman/listinfo.cgi/distsec**

Working within IETF

- **If I were to take OGF firewalls work to IETF today, I would:**
  - **Engage distsec mailing list**
  - **Submit well-defined, clearly scoped and constrained requirements with clear use cases**
  - **Talk to Security Area directors**
  - **Engage EMERG -- contact chairs**

A little about what we're doing at Cisco

- **Focusing on firewall control**
- **Consistent authorization environment across technologies**
- **Assumptions/values**

  We *can* change the firewall

  We *must* allow the firewall to do its job

  Don't allow or enable bypass of firewall policy enforcement

  – **Granularity of authorization**

  Performance matters

  – **Minimize "post-dial delay"**

  – **Headergrams are bad**

  Give the network administrator the tools he/she needs to control network boundaries

Off-path firewall control at Cisco

- **Authorized Firewall Control Application**

  Based on general-purpose authentication & authorization framework

  Prototype implemented in IOS

  http://www.ietf.org/internet-drafts/draft-shore-afwc-00.txt

On-path firewall control at Cisco

- **Network-Layer Signaling**
  - **On-path signaling protocol**
  - **NAT traversal support in transport layer**
  - **Picked up by PacketCable as transport for discovery protocols**
  - **Implemented in IOS, shipping next year**
  - **Requesting IETF publication as informational RFC**
  - **http://www.ietf.org/internet-drafts/draft-shore-nls-tl-03.txt**
  - **Firewall application written, probably not going to pursue it**
  - **http://internet-drafts.osmirror.nl/draft-shore-nls-fw-00.txt**