FiTP –

Comments to draft protocol seen so far

r.niederberger@fz-juelich.de

Request for Comments

- Security-Area (at) OGF
  - Jan Just Keijser NICHEF.nl
- Infrastructure-Area (at) OGF
  - FVGA-WG (2 replies)
  - NML-WG (-)
  - NM-WG (-)
  - NSI-WG (-)
  - OCCI-WG (3 replies)
- Melinda Shore (Cisco and IETF MIDCOM WG)
- Magnus Westerlund (IESG member)

Responses by OCCI

Responses from **Open Cloud Computing Interface** (OCCI-WG)

1. perhaps the BEHAVE WG [1] might be a useful port of call. They aim to introduce and track "best current practices to enable NATs to function in as deterministic a fashion as possible."
2. Why isn't one of uPNP, STUN, SOCKsv4/v5 (IETF authenticated firewall traversal), or SPP good enough? uPNP has horrible security, but it's otherwise a good protocol. If you fixed that, it would be great. And IETF BEHAVE has done a lot of work.

Behavior Engineering for Hindrance Avoidance (behave)

- http://www.ietf.org/html.charters/behave-charter.html
  ======================================
  The behavior of NATs varies from one implementation to another. As a result it is very difficult for applications to predict or discover the behavior of these devices. Predicting and/or discovering the behavior of NATs is important for designing application protocols and NAT traversal techniques that work reliably in existing networks. This situation is especially problematic for end-to-end applications where one or both end-points are behind a NAT, such as multiuser games, interactive multimedia and P2P download.

  The working group documents best current practices to enable NATs to function in as deterministic a fashion as possible. The NAT behavior practices will be application independent. This has already completed for UDP, TCP, DCCP, Multicast and ICMP. It continues with SCTP and any additional protocol deemed necessary to handle. The WG has documented approaches for characterizing and testing NAT devices.

  BEHAVE will develop protocol-independent toolkits usable by application protocols for NAT traversal. … It will now produce a relay protocol that focuses on security that is usable with both IPv4 and IPv6, and capable of relaying between the two IP versions. ….
  …..
  Translation mechanisms cannot transparently support protocols that embed network addresses within their protocol messages without ALGs. Because ALGs have security issues …, are error prone and brittle, and hinder application development, the usage of ALGs in the defined translators should be avoided. ….

UPnP, STUN, SOCKS

- http://de.wikipedia.org/wiki/Universal_Plug_and_Play
  ======================================
  Though for equipment requireing to make known to the network. Uses Multicast to do so. A grid server could do this to becom eknown by a FW. But does not help to authenticate/authorize user clients.

- http://de.wikipedia.org/wiki/STUN
  ========================
  STUN (= *Session Traversal Utilities for NAT*, RFC-5389)
  uses UDP and an external server, which knows official addresses (see skype)
  "STUN is not a NAT traversal solution by itself. Rather, it is a tool to be used in the context
  of a NAT traversal solution. This is an important change from the previous version of this
  specification (RFC 3489), which presented STUN as a complete solution.„

- http://de.wikipedia.org/wiki/SOCKS
  ==========================
  IETF authenticated firewall traversal (RFC 1928)
  Uses proxy server, which has to be installed and managed.(slow and inefficient)

Response from Melinda Shore

Melinda Shore

(Cisco Systems and former Chair of IETF MIDCOM group)

- OGF has an interesting set of requirements that have some overlap with more general distributed computing policy issues, particularly around inter-organizational policy.
- They also have some policy services that the IETF does not.
- I do think that this work does not overlap very much with existing or past IETF work and there may be some synergy with some of the discussions that crop up from time to time about v6 firewalling even though the OGF operates mostly in a v4 environment.

Middlebox Communication (midcom)

http://www.ietf.org/html.charters/midcom-charter.html

As trusted third parties are increasingly being asked to make policy decisions on behalf of the various entities participating in an application's operation, a need has developed for applications to be able to communicate their needs to the devices in the network that provide transport policy enforcement. Examples of these devices include firewalls, network address translators (both within and between address families), signature management for intrusion detection systems, and multimedia buffer management. These devices are a subset of what can be referred to as 'middleboxes.'

This working group will focus its attention on communication with firewalls and network address translators (including translation between IPv6 and IPv4). Work will not preclude extensibility to other categories of middle box.
…
This working group will concern itself with an environment that consists of:
- one or more middle boxes in the data path
- an external requesting entity
- a policy entity for consultation purposes when the requesting entity is untrusted.

…..

…..

Rechartered to get application complexity out of middleboxes

Response from Magnus Westerlund

magnus.westerlund (at) **ericsson.com** (IESG Member 2009 / Transport)

- The NSIS WG has ongoing work, requested to be published on NAT and Firewall control. http://tools.ietf.org/wg/nsis/ http://tools.ietf.org/wg/nsis/draft-ietf-nsis-nslp-natfw /
- Otherwise there isn't much ongoing in IETF for Firewall control. There is a bit more discussion about doing something else when it comes to NATs. However, there is currently no chartered work yet.
- There is some discussion in BEHAVE WG focused on NATs.
- There are more discussion ongoing in the v6ops WG related to firewall for IPv6, especially in the context of consumer premise equipment. http://tools.ietf.org/wg/v6ops/
- For example Apple has an individual proposal for a simple firewall control protocol. http://tools.ietf.org/html/draft-woodyatt-ald-03
- If you want a more targeted group of people for review I think Melinda can help you. Your work looks interesting. I think we are definitely interested in learning what requirements that you see. When it comes to review I can't commit anyone as we are an volunteer organization. But there is likely a few interested.

Response from Jan Just Keijser

janjust@nikhef.nl (Security Area)

- the routers/firewalls between the client and the FiTP server are supposed to "snoop" the traffic to look for FiTP exchange messages. But how would a router/firewall tell either the client or the server that a particular request is not possible/not granted? Where is the error recovery?
- How does the FiTP protocol deal with NATting, especially in a 1-to-many NATting setup.
- Wouldn't it make more sense to have the FiTP server send complete instructions back to the client?

Questions and discussion