Internet Draft
Expiration Date: August 2000

B. Biggs
3COM

March 2000

A SIP Application Level Gateway for Network Address Translation
draft-biggs-sip-nat-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as work in progress.

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document describes an Application Level Gateway (ALG) for the Session Initiation Protocol (SIP) by which IP addresses in the SIP message and in the SDP body are statically mapped from one group to another. The SIP ALG is a specific case of an Application Level Gateway as described in [1].

Transparent use of SIP-based devices in a Network Address Translation (NAT) scenario requires that modifications be made to the SIP messages. These modifications are performed by the ALG.

Table of Contents

1. Introduction

The need for IP address translation arises when a network's internal IP addresses cannot be used outside the network either for security reasons or because they are invalid for use outside the network. Use of network address translation devices allows local hosts on such private networks to transparently access the external global Internet and enables access to selective local hosts from the outside. This solution is becoming widely popular due to the scarcity of IPv4 addresses.

The Session Initiation Protocol (SIP) [1] is a signalling protocol for the setup of multimedia sessions across the Internet. The protocol itself makes extensive use of network addresses located inside the message body, making it impossible to use SIP through basic network address translation without an Application Level Gateway (ALG).

Full support of SIP by a firewall or NAT device is a difficult task. It requires near full message parsing, and knowledge of call state to know when to terminate media flow. It requires full encryption and authentication support, and possibly the ability to generate its own responses. However, in many situations this is neither feasible nor required.

This document describes an implementation of a minimal SIP ALG for the purpose of allowing simple SIP sessions to pass through a NAT device. Rather than attempt to tackle the full SIP specification, we have chosen a subset of the functionality which we feel is sufficient for typical use. In section 2, we outline what scenarios we believe that this method will be appropriate. Section 3 describes in sufficient detail what tasks a SIP ALG must perform.

Note that this ALG is currently only discussing an implementation for UDP SIP traffic, and that the modifications required to support TCP are currently unknown. As well, this ALG only describes modifications for implementations which use SDP to describe the media stream.

2. Problem Scope and Requirements

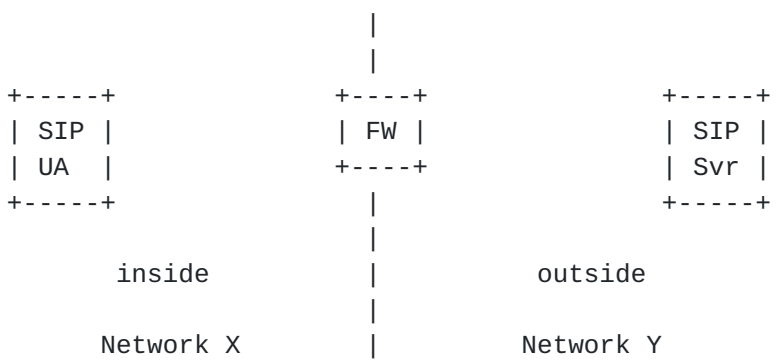

Figure 1: External Service [2]

The ALG framework described is designed to specifically solve the problem of SIP User-Agents behind a firewall communicating with SIP entities located outside of the firewall. In this document, we refer to outgoing messages as being messages from inside the private network traveling outside to the public Internet, and incoming messages as the opposite.

This scenario is described in the SIP Firewalls draft [2] as 'External Service'.

A SIP message is identified by the ALG by using port 5060 as the destination. Most NAT implementations identify the type of traffic they will modify by using the port as an identifier, so this restriction seems practical.

It is assumed that in a typical NAT situation, if a host on the internal network attempts to send a UDP message at random to a host located on the public Internet, that the packet will be modified to appear as if it came from the firewall host and sent unmodified on its way. This seems to be the typical scenario for most NAT environments. This assumption is important because it implies that we do not need to setup mappings to allow for media to be sent from

internal hosts to external SIP agents.

In cases where the above assumption is not valid, note that incoming SDP must be modified and an additional port mapping be created.

3. Translating IP Addresses in SIP Messages

This section describes the areas of the SIP message which need to be checked for addresses requiring translation.

A general SIP ALG must be capable of modifying the data in both the incoming and outgoing packets. Specifically, for outgoing SIP messages the headers which must be modified are the Via, Contact and Content-Length headers. If the body of the data is of type 'application/sdp'. then it must also be modified. For incoming messages, the only required modification is the SDP body.

In general, the NAT device maintains a table of port mappings which allow ports on the globally routable address to map back to hosts and ports behind the device.

For SIP messages, we propose that an ALG designate a single port for each SIP device behind the firewall, and setup mappings as required for media which flows through.

3.1 Outgoing SIP Message Modifications

When an outgoing SIP message is encountered, the ALG must first lookup to see if there already exists a port mapping for the SIP UA. A complete ALG should do a lookup based on the address listed in the maddr field of the Via, and otherwise the address of origin of the packet, and the port listed in the Via.

If a port mapping does not already exist, a port must be chosen to allow for incoming SIP responses and future requests to be sent back to the SIP UA behind the firewall. Due to the nature of SIP, this port mapping must not be associated with a remote IP address. Any external host must be able to use the port mapping to reach the SIP UA behind the Firewall.

Most NAT implementations use a timeout for UDP port mappings. In the case of this SIP signalling port, the timeout must be increased to an appropriate amount. We believe that a timeout of at least one hour is sufficient to allow most phones to send a REGISTER message to the

external proxy.

3.1.1 Modifying the Topmost Via Header

If the outgoing message is a SIP request, the Via must first be modified such that responses to the request will get sent to the NAT host on a port which is mapped to the appropriate client. This involves modifying the port listed in the topmost Via. If the Via contains an maddr field, this must be replaced by the IP address of the NAT device. Otherwise, it is usually safest to modify the IP address in either the received tag if one exists, or simply the address in the sent-by.

3.1.2 Modifying the Contact Header

The Contact header must also be modified to reflect the NAT mapping to ensure that future SIP requests will get sent to the appropriate SIP UA.

3.1.3 Modifying the SDP Body

If the body of the SIP request is of type 'application/sdp', then it must be checked for address information to be modified.

This first involves modifying the 'c=' line to reflect the IP address of the NAT device. Note that if the address listed in the 'c=' line is the null address (0.0.0.0), then this signifies that the call is on hold, and no mangling needs to be performed on the SDP.

For each 'm=' line in the body, a port mapping must be setup for incoming packets and the port changed in the SDP message. The timeout on these ports must last for at least a few minutes to allow for a reasonable delay in call setup. The port mapping must not be bound to any external IP address, since media can come from anywhere.

It's also important to note that RTP port mappings must be on an even numbered port on the NAT host, and that the port numbered one higher must also be forwarded for RTCP.

As with the SIP signalling port mapping, the mapping setup for incoming media must not impose future restrictions on where media is to come from. Other hosts on the Internet must be able to send to the same port on the NAT device and reach the same destination behind the firewall.

3.1.4 Modifying the Content-Length Header

If the SDP body has changed due to a port mapping being setup, then

the Content-Length header of the SIP message must be changed to reflect the new length.

3.2 Incoming SIP Message Mangling

An optimization can occur when two SIP User Agents both behind the firewall make a call to each other. In order to avoid having media between two internal hosts flow through the NAT host, incoming SIP messages must be checked to ensure that the address of the NAT host is not present in the SDP body.

If the body of the SIP message is of type 'application/sdp', then the NAT host should check for its own address listed in the 'c=' line. If it is a match, then each 'm=' line should be checked to find existing port mappings. When a match is found, the 'c=' line and all 'm=' lines should be modified to reflect the internal hosts.

4. Example Message Translation

In the following message example, we will only show some of the relevant headers for address translation purposes.

In this example, a client 10.0.0.99 attempts to call a phone on the Internet at address billy@3com.com. In this example, C is the client, P is the proxy on the Internet.

```
C->P: INVITE sip:billy@3com.com SIP/2.0
      Via: SIP/2.0/UDP 10.0.0.99
      Call-ID: 30309090808@10.0.0.99
      Contact: <sip:10.0.0.99>
      Content-Type: application/sdp
      Content-Length: 107

      v=0
      o=username 0 0 IN IP4 10.0.0.99
      c=IN IP4 10.0.0.99
      t=0 0
      m=audio 4330 RTP/AVP 0
```

This message is the intercepted by the ALG with an address of 149.112.117.203, which sets up a port mapping at port 60080 to map back to the phone behind it for SIP messages, and also sets up a port mapping on port 60082 to allow for incoming media to be sent again back to the phone. A port mapping on port 60083 for RTCP is also created. It then translates the packet to look as follows:

```
N->P: INVITE sip:billy@3com.com SIP/2.0
      Via: SIP/2.0/UDP 149.112.117.203:60080
      Call-ID: 30309090808@10.0.0.99
      Contact: <sip:149.112.117.203:60080>
      Content-Type: application/sdp
      Content-Length: 114

      v=0
      o=username 0 0 IN IP4 10.0.0.99
      c=IN IP4 149.112.117.203
      t=0 0
      m=audio 60082 RTP/AVP 0
```

N represents the NAT host. Note that the address in both the Call-ID and the 'o=' line of SDP do not need to be changed to reflect the mapping, since they are only used for global uniqueness. It is assumed that uniqueness will more than likely be preserved anyways.

5. Security Considerations

There are many security concerns about NAT systems in general, especially ones which require that port mappings be setup allowing any Internet host to send random UDP traffic through a firewall.

Attackers from the Internet could inflict denial of service attacks to many phones simply by blasting traffic at a range of ports known to likely map back to SIP devices. Since no remote IP address can be set on media streams, a malicious user can blast unsolicited audio at many phones simply by directing its attack on a range of ports known to be reserved for NAT.

6. Current Implementations

A basic SIP ALG was implemented at 3Com using the Linux IP masquerading system. Source code for this module is available at:

http://www.sip-happens.com/masquerade/

7. References

[1] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: session initiation protocol," Request for Comments (Proposed Standard) 2543, Internet Engineering Task Force, Mar. 1999.

[2] J. Rosenberg, D. Drew, H. Schulzrinne, "Getting SIP through Firewalls and NATs," Internet Draft, Internet Engineering Task Force, Feb. 2000. Work in progress.

[3] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

Acknowledgements

Thanks goes to Rick Dean, Jacek Grabiec, Jerry Mahler, and Guido Schuster.

Authors' Addresses

Billy Biggs
3COM
3800 Golf Rd
Rolling Meadows, IL
USA

Phone: +1 847 262-2561
EMail: Billy_Biggs@3com.com
URI: http://www.3com.com/