Network Working Group
Internet-Draft
Expires: May 20, 2008

Q. Xie
Motorola
R. Stewart
Cisco Systems, Inc.
M. Holdrege
Strix Systems
M. Tuexen
Muenster Univ. of Applied Sciences

November 17, 2007

SCTP NAT Traversal Considerations
draft-xie-behave-sctp-nat-cons-03.txt

Status of this Memo

Copyright Notice

Abstract

This document defines and classifies scenarios for the usage of SCTP in networks with NATs and similar middleboxes.

Table of Contents

1. Conventions

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

2. Introduction

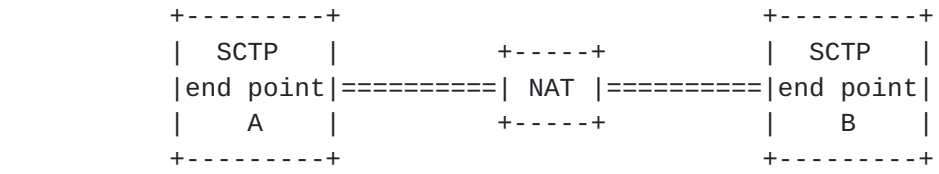
It is the job of Network Address Translators (NAT) [RFC2663] and middleboxes [RFC3304] that utilize a NAT function to manipulate address and port information in the IP and transport header. This poses a challenge for hosts that attempt to use certain end-to-end protocols [RFC3027]. This issue has drawn increasingly wide attention from the IP development and service community and much work has been done to ameliorate the situation for UDP, TCP and other protocols.

The same issue not only exists for SCTP [RFC4960], but also may become a more difficult issue when SCTP associations are multi-homed. This document defines and classifies scenarios dealing with SCTP and NAT traversal. In the following discussion, we will simply refer to NAT as a function, but note that many types of middleboxes employ NAT functions.

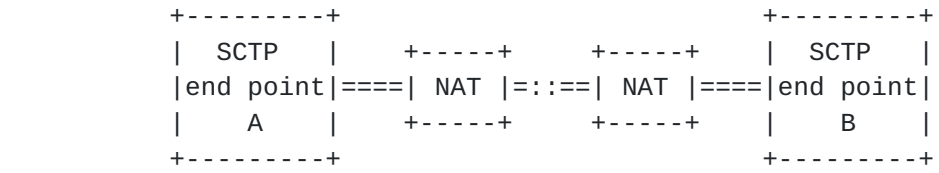
3. SCTP NAT Traversal Scenarios

3.1. Single Point Traversal

In this case, all packets in the SCTP association go through a single NAT, as shown below:



A variation of this case is shown below, i.e., multiple NATs in a single path:

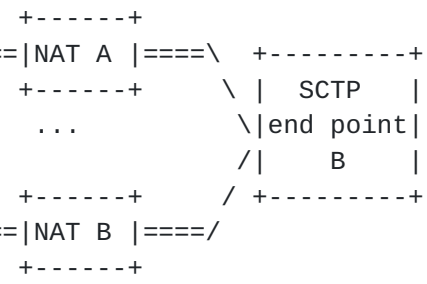


The two SCTP endpoints in this case can be either single-homed or multi-homed. However, the important thing is that the NAT (or NATs) in this case sees ALL the packets of the SCTP association.

In this single traverse point scenario, we must acknowledge that while one of the main benefits of SCTP multi-homing is redundant paths, the NAT function represents a single point of failure in the path of the SCTP multi-home association. However, the rest of the path may still benefit from path diversity provided by SCTP multi-homing.

3.2. Multi Point Traversal

This case involves multiple NATs and each NAT only sees some of the packets in the SCTP association. An example is shown below:



This case does NOT apply to a singly-homed SCTP association (i.e., BOTH endpoints in the association use only one IP address). The advantage here is that the existance of multiple NAT traverse points can preserve the path diversity of a multi-homed association for the entire path. This in turn can improve the robustness of the communication.

To make this work, however, all the NATs involved must recognize the packets they see as belonging to the same SCTP association and perform address translation in a consistent way. It may be required that a pre-defined table of ports and addresses would be shared between the NAT's. Other external management schemes that help multiple NAT's coordinate a multi-homed SCTP association could be investigated.

4. Considerations for SCTP NAT Traversal

In any type of traverse, the NAT must understand the SCTP protocol. Since SCTP is relatively new (compared to UDP or TCP), some older existing NATs that are capable of handling UDP or TCP traverse will need to be enhanced for SCTP. In this section we discuss what considerations should be made for that NAT enhancement.

In a single-homed SCTP association, each endpoint uses only one IP address and the association will always go through a single NAT traverse point. It is important that the endpoints do not list the IP-address again within the INIT or INIT-ACK chunks when setting up the association. This makes sure that the NAT engine is not required to change the INIT or INIT-ACK chunk when modifying the IP-addresses of the packets containing the INIT and INIT-ACK chunks.

It is also important that the checksum of the whole SCTP packet has to be recalculated if a part of the SCTP packet, for example port numbers or IP-addresses listed in the INIT or INIT-ACK chunk, is modyfied. It is not possible for the SCTP checksum to calculate the difference of the checksum based only on the difference of the packets like it is possible for the checksum used for TCP or UDP.

5. Security Considerations

See [RFC4960] on SCTP security considerations.

6. References

6.1. Normative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Informative References

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC3027] Holdrege, M. and P. Srisuresh, "Protocol Complications with the IP Network Address Translator", RFC 3027, January 2001.

[RFC3304] Swale, R., Mart, P., Sijben, P., Brim, S., and M. Shore, "Middlebox Communications (midcom) Protocol Requirements", RFC 3304, August 2002.

[RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

Authors' Addresses

Qiaobing Xie
Motorola, Inc.
1501 W. Shure Drive, 2-F9
Arlington Heights, IL 60004
USA

Phone: +1-847-632-3028
Email: qxie1@email.mot.com

Randall R. Stewart
Cisco Systems, Inc.
4875 Forest Drive
Suite 200
Columbia, SC 29206
USA

Email: rrs@cisco.com

Matt Holdrege
Strix Systems
Suite 110, 26610 Agoura Road
Calabasas, CA 91302
USA

Email: matt@strixsystems.com

Michael Tuexen
Muenster Univ. of Applied Sciences
Stegerwaldstr. 39
48565 Steinfurt
Germany

Email: tuexen@fh-muenster.de

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).