Elektrotehniški vestnik 75(5): 277-284, 2008
Electrotechnical Review: Ljubljana, Slovenija

SCTP association between multi-homed endpoints over NAT using NSLP

Tine Stegel, Janez Sterle, Janez Bešter, Andrej Kos

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška 25, 1000 Ljubljana, Slovenia
E-pošta: tine.stegel@fe.uni-lj.si

Extended abstract. Network address translation poses a challenge for hosts that attempt to use protocols that place internet protocol addressing information inside IP payload. The same issue exists for the Stream Control Transmission Protocol and is even more difficult when SCTP associations are multi-homed. This paper deals with the options available for establishment of an SCTP association between multi-homed endpoints with multi-point NAT traversal on both sides and stress imposed limitations, when a single-point NAT traversal is used instead. We will discuss a unique problem that SCTP introduce with multi-homing, which is port preservation over an entire SCTP association even if it traverses multiple NATs. Most of the existing traversal techniques do not cover synchronizing multiple NATs and are therefore inappropriate for SCTP. Finally, we will show how the NAT/Firewall NSIS Signaling Layer Protocol can be used for reserving the port number, acquiring public addresses and opening data flows over NATs that are included in the SCTP association.

Keywords: SCTP, Multi-homing, NAT, Multi Point Traversal, NSLP

Povezava SCTP med večdomnima končnima točkama s prečkanjem NAT in uporabo protokola NSLP

Povzetek. Prevajanje naslovov IP NAT je izziv za vse protokole, ki naslove IP prenašajo tudi v svojih podatkovnih enotah. SCTP se poleg omenjenega problema sooča tudi z izzivom večdomnosti, ki uvede potrebo po usklajevanju vseh naprav NAT, ki sodelujejo pri povezavi SCTP. V članku smo raziskovali postopke, ki so na voljo za vzpostavitev povezave SCTP med večdomnima končnima točkama z enokratnim ali vzporedno večkratnim prečkanjem NAT. Obravnavali smo problem zagotavljanja iste številke vrat pri vseh vzporednih napravah NAT, saj povezavo SCTP poleg liste izvornih naslovov IP definira le ena številka vrat na vsaki strani. Večina obstoječih rešitev za prečkanje NAT ne predvideva usklajevanja različnih naprav NAT, zato tudi niso primerna za uporabo pri SCTP. V članku bomo prikazali uporabo protokola NAT/Firewall NSIS Signaling Layer Protocol, ki ga končna točka SCTP lahko uporabi za rezervacijo številke vrat, poizvedbo o javnih naslovih IP, ki se uporabljajo pri vsakem prevajanju, ter odprtju podatkovnega toka v smeri iz javnega omrežja v zasebno omrežje.

Ključne besede: SCTP, večdomnost, NAT, vzporedno večkratno prečkanje, NSLP

1 Introduction

The Stream Control Transmission Protocol (SCTP) [1] is a new transport protocol that comprises both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) features and further enhances end-to-end connectivity with multi-homing, multi-streaming and selective acknowledgment. SCTP endpoints can use several source internet protocol (IP) addresses. This means that, if the network topology allows, they can be reachable via different network paths. To utilize this multi-homing option, SCTP endpoints must exchange their lists of source IP addresses in the initial four-way hand shake or later add them with the Address Configuration Change mechanism [2]. Network Address Translators (NAT) [7] and middleboxes that utilize a NAT function manipulate address and port information in the IP and transport header. This poses a challenge for hosts that attempt to use end-to-end protocols that also place IP addressing information inside IP payload. The same issue exists also for SCTP and becomes a more difficult one when SCTP associations are multi-homed. This paper will research the options that are available to establish a multi-homing SCTP association with a single or multiple NAT on its multiple network paths.

SCTP is commonly used by newly defined protocols that need a reliable high performance transport. For example, the upper layer protocols in Signaling Transport protocol stack (SIGTRAN) [21], DIAMETER [22] and also Session Initiation Protocol (SIP) [23] [24] can use SCTP instead of TCP. As these protocols cover environments that can comprise both public and private realms, NAT issues can be resolved as discussed in the paper.

Received 4 March 2008
Accepted 27 June 2008

There have been several papers published on research in the use of SCTP for horizontal and vertical soft handovers [16] [17] [18]. Research for concurrent multipath transfer for better performance under network failures has been done for various environments including battlefield networks [19]. Some suggestions like Load Sharing - SCTP (LS-SCTP) [8] have also been made to improve SCTP so as to support load sharing using all paths for data transmission. Further research on handovers, concurrent multipath transfer and load sharing with SCTP could be extended with NAT traversal as proposed in our paper.

2 SCTP Association

2.1 Initialization of SCTP Association

During the initialization of the SCTP association, four messages are exchanged as shown in Figure 1. The initiator sends the INIT chunk that contains a list of endpoint source IP addresses and waits for the same information from the responder INIT ACK chunk. The endpoints port number is always present in the SCTP header. Connection is later confirmed with COOKIE ECHO and COOKIE ACK chunks that finalize the verification and establishment procedure. If there is no IP address present in INIT or INIT ACK chunk, the source IP address from IP header is used by the receiving SCTP endpoint. SCTP association is defined with one list of IP addresses and one port number for each SCTP endpoint [1].

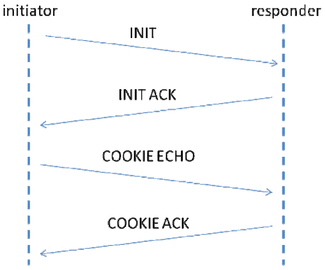

Figure 1. SCTP initial four way handshake.

Slika 1. SCTP začetna izmenjava 4 sporočil.

2.2 SCTP Dynamic Address Reconfiguration

The SCTP dynamic address reconfiguration mechanism can be used for dynamic addition and subtraction of IP addresses in SCTP association. When one SCTP endpoint wants to add an IP address, it sends an Address Configuration Change Chunk (ASCONF) that must be acknowledged with an Address Configuration Acknowledgment Chunk (ASCONF-ACK). The procedure is shown in Figure 2.

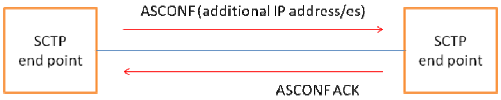

Figure 2. Address Configuration Change procedure.

Slika 2. Dinamično dodajanje naslovnih parametrov

3 Network Address Translation

NAT devices translate IP addresses in private address ranges into public addresses when traffic traverses between the private and public networks. Basic NAT and NAPT are two variations of traditional NAT. Basic NAT is limited to IP addresses alone, whereas translation in Network Address Port Translation (NAPT) is extended to include IP address and Transport identifier (such as TCP/UDP port or ICMP query ID) [7]. In this paper we focus on NAPT and therefore whenever the NAT term is used it should be understood as NAPT. NAT is often accompanied by application-specific gateways (ALGs) for performing additional alterations of the payload data.

There are different types of NAT implementations like full cone, (address) restricted cone, port restricted cone and symmetric NAT. Several NATs attempt to use the same external port number as the one used by the internal host. This is referred to as port preservation [20]. However, if two internal hosts attempt to communicate with the same external host using the same port number, the external port number used by the second host will be different. Some of the NATs that do this were found to have different characteristics depending on whether the port was already in use or not [20]. If the port is preserved, the most commonly used NAT behavior is the port-restricted cone and full cone. If the port cannot be preserved, usually the same behavior is used as with port preservation although on some occasions symmetric NAT is used.

Symmetric NAT is the most complex and difficult to use in communication, since each request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source port and IP address. As some of the proposed solutions given in this paper have problems with symmetric NAT, limitations are pointed out wherever they are any.

4 Multi-Homing and NAT

An SCTP endpoint is considered multi-homed if there are more than one IP address that can be used as a destination address to reach that endpoint. One of the multiple destination addresses of a multi-homed peer endpoint is selected as the primary path and is always used for transmission, unless the SCTP user explicitly specifies the destination IP address (and possibly source IP address) to use. An SCTP endpoint monitors the reachability of the idle destination IP address(es) of its peer by sending a HEARTBEAT chunk periodically to the destination IP address(es). With that knowledge SCTP endpoint can immediately replace the primary path with an alternative active path in case of failure. Multi-homing functionality works without additional signaling, if there is no network address translation along the path between the endpoints.

To fully exploit the benefits of multi-homing, the network topology has to offer the possibility to physically separate multiple paths used in SCTP association. For that purpose, if using NAT, SCTP endpoint should be reachable through more NAT devices that are physically separated. Additional signalization is therefore necessary to coordinate synchronous operation of all included NATs. Network address translation changes private IP addresses to public IP addresses and therefore hides the private addresses to any public host. SCTP endpoint can communicate with the other peer only through public addresses of NAT devices and furthermore, only if NAT bindings have been activated in advance.

Three major issues have to be resolved. The first one is discovering the public IP address used at every translation, the second one is reserving the same port number used at every translation and the third one is the activation of the NAT address binding at the destination edge NAT, so that INIT chunk can get to the other peer behind NAT. If a multi-point traversal is used, NAT address bindings must be coordinated also on all other included NATs on both sides.

5 SCTP NAT Traversal Scenarios

5.1 Single Point Traversal

Endpoints behind NAT that have only one access to the public network, t.i. via one NAT, are represented outside with only one public IP address. The topology is presented in Figure 3. Even if endpoint is multi-homed in its private network, it cannot use more than one source IP address, since NAT would translate all different private IP addresses into one public IP address and assign a different port number for each binding, which is unacceptable for SCTP association. Endpoints that are not behind NAT can use more source IP addresses, with the same port number.

Although single-point traversal nullifies the multi-homing option in a private network behind NAT, SCTP association can still benefit from the multi-homed SCTP endpoint in a public network. Initiator behind NAT can choose not to send any IP addresses in the INIT or INIT ACK chunk. That forces the endpoint which receives this initiation message to use the source address in the IP header as the only destination address for this association [5].

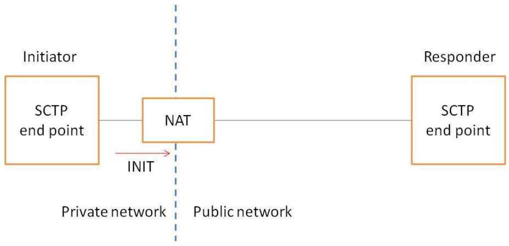

Figure 3. Initiating SCTP endpoint in private network behind NAT.

Slika 3. SCTP končna točka v privatnem omrežju za NAT začne z vzpostavljanjem SCTP povezave.

Responder sends its IP address list in INIT ACK chunk. Reception and usefulness of this information depend on the type of NAT. INIT ACK chunk should be sent from the same IP address found in the IP header of the received INIT chunk. Furthermore, any communication to other still unused IP address has to be started from the private realm. If NAT is symmetric, every time different destination IP address from the IP address list found in INIT ACK chunk is used, a new port number is assigned when traversing NAT. Single traversal with symmetric NAT therefore cannot utilize multi-homing in SCTP association.

Responder behind NAT as presented in Figure 4 or Figure 5 has to achieve a NAT mapping that enables outsider to initiate an association. NAT can be preconfigured or some protocol can be used for its remote adjustment. Same limitations as described above are present for different types of NAT.

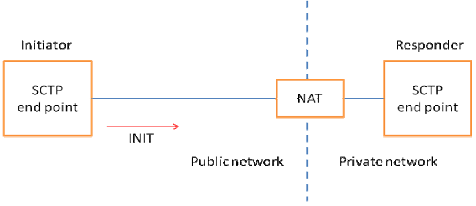

Figure 4. Responding SCTP endpoint in private network behind NAT.

Slika 4. Odgovarjajoča SCTP končna točka v privatnem omrežju za NAT.

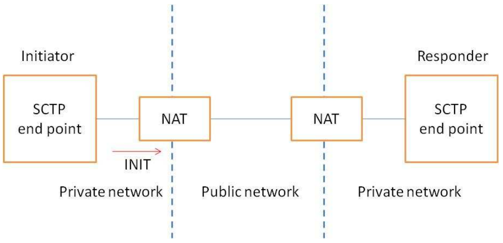

Figure 5. Network address translation on both sides.

Slika 5. NAT na obeh straneh.

5.2 Multi Point Traversal

This case involves multiple NATs, where each NAT only sees some of the packets in SCTP association. Topology is presented in Figure 6 and Figure 7. Distributed NATs are required to translate all SCTP messages of one SCTP association using the same source port number. Even if SCTP endpoint is multi-homed, it only has one port number [1]. This port number can be changed with NAT, but only if all the included NATs make the same change. Without static configuration or synchronizing NATs with additional signalization it is very difficult to fully initialize multi-homed SCTP association. It might be possible to count on a port preservation rule [20] on NATs, which advise them to use the same port number in both realms if possible, but this solution is unpredictable.

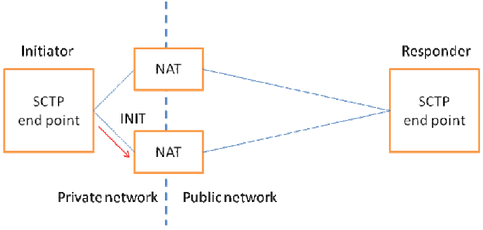

Figure 6. Multi-point traversal on initiator side.

Slika 6. Vzporedno večkratno prečkanje NAT na vzpostavitveni strani.

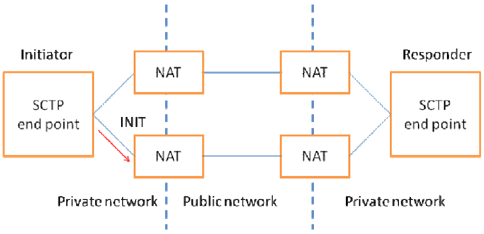

Figure 7. Multi-point traversal on both sides.

Slika 7. Vzporedno večkratno prečkanje NAT na obeh straneh.

An additional problem is translating the entire list of source IP addresses in INIT or INIT ACK chunk. Since NAT is only aware of its own public IP address, it does not know about other NATs public addresses. Therefore, ALG that is usually used for altering payload data can only substitute one IP address in the source IP list with the one found in the IP header. Since all the remaining addresses in the list are still private, the list is of no use for the receiving SCTP endpoint. Informing all NATs about all pairs of private/public mappings seems too complicated; therefore SCTP endpoint has two options. It can choose not to send IP addressing information in the payload or it can learn NATs' public IP addresses and make appropriate adjustments to INIT and INIT ACK chunks before sending them.

In the first case, the SCTP association should first be established with an empty INIT chunk and later an empty ASCONF chunk should be used to add an additional IP address in the SCTP association. If ASCONF chunk does not include any address, IP address from the IP header is used instead, which is the public IP address of traversed NAT. The sender would have to take special care of sending the ASCONF chunk via the intended NAT. If port preservation is not succeeded, SCTP association can be restarted with another source port number or be used as single-homed.

In the second case, SCTP endpoint has to use other means to learn public addresses of all the used NATs. With that information it can generate an INIT chunk that comprises a list of public IP addresses that is still packed in an IP packet having a private source IP address in the IP header. The problem of this solution is that other NATs, where INIT chunk has not passed, are still closed and sending HEARTBEAT chunks to those public addresses will not be successful. NAT bindings can be activated statically or using protocols that can dynamically configure NAT.

5.3 Symmetric NAT Limitations

As discussed above, using single-traversal with symmetric NAT cannot utilize multi-homing. Although multi-homing can be utilized using multiple-traversal, deployed network topology has to follow strict rules. When using symmetric NAT, one NAT device can be a part of only one SCTP path. If a NAT device were a part of multiple SCTP paths, a different port number would be used at the traversal for each path, which is unacceptable for SCTP.

If NAT is used only on one side, a public SCTP endpoint can use only as many public addresses as the private SCTP endpoint has NAT devices that connect it to the public network. If NAT is used on both sides, the number of NAT traversals has to be identical on both sides.

6 NAT Traversal Techniques

Several solutions to enable applications to traverse firewall or NAT have been proposed and are currently in use [13]. Typically, application level gateways (ALG) have been integrated with the firewall or NAT to perform the application layer functions required for a particular protocol to traverse a NAT. Typically, this involves rewriting application layer messages to contain translated addresses, rather than the ones inserted by the sender of the message [11].

Another approach is middlebox communication (MIDCOM) [14], where ALGs external to the firewall or NAT configure the corresponding entity via the MIDCOM protocol. We already discussed ALG's lack of information that is needed for all correct alternations of multiple IP addresses in the payload and its inability to synchronize itself with multiple ALG entities on different NAT devices to use the same port number.

Therefore, we concluded that when using SCTP with multi-homing, ALGs can be of a very limited use.

Several other work-around solutions are also available, such as STUN [11]. STUN defines the binding method used by a client to determine its reflexive transport address towards the STUN server. The reflexive transport address can be used by the client for receiving packets from peers, but only when the client is behind specific types of NATs. STUN does not work with symmetric NAT [11] and it would also not work with multi-homed SCTP since it cannot guarantee the same port number on multiple NATs. An extension to STUN, called TURN [9], allows a client to request an address on the TURN server, so that the TURN server acts as a relay. This extension defines a handful of new STUN methods. Although a relayed transport address is highly likely to work when corresponding with a peer, it comes at high cost to the provider of the relay service. Protocols using relayed transport addresses should make use of mechanisms to dynamically determine whether such an address is actually needed. One such mechanism, defined for multimedia session establishment protocols based on the offer/answer protocol, is Interactive Connectivity Establishment (ICE) [15].

Most of these approaches introduce other problems that are generally hard to solve, such as dependencies on the type of NAT implementation (full-cone, symmetric, etc), or dependencies on certain network topologies. What is even more important for SCTP, they lack mechanisms to support multi-homed endpoints.

7 NAT/Firewall NSIS Signaling Layer Protocol

The NAT/Firewall NSIS Signaling Layer Protocol (NAT/Firewall NSLP) [3] is a path-coupled signaling protocol for an explicit Network Address Translator and firewall configuration within an extensible IP signaling framework currently being developed by the IETF Next Steps in Signaling (NSIS) working group. This new protocol is designed to request the dynamic configuration of NATs and/or firewalls along the data path. Dynamic configuration includes enabling data flows to traverse these devices without being obstructed, as well as blocking of particular data flows at inbound firewalls. Enabling data flows requires the loading of firewall rules with an action that allows the data flow packets to be forwarded and creating NAT bindings. Signaling must reach any device on the data path that is involved in. This means that it is convenient if signaling travels path-coupled, meaning that the signaling messages follow exactly the same path that the data packets take.

NATFW NSLP is carried over the General Internet Signaling Transport (GIST, the implementation of the NTLP) defined in [4]. NATFW NSLP messages are initiated by the NSIS initiator (NI), handled by NSIS forwarders (NF) and received by the NSIS responder (NR). For the purposes of this paper let us suppose that NI and NR are the SCTP endpoints establishing a SCTP association. Every NATFW NSLP-enabled NAT along the data path intercepts these messages, processes them, and configures itself accordingly. Thereafter, the actual data flow can traverse all these configured NATs. It is assumed that NATs will be statically configured in such a way that NATFW NSLP signaling messages are allowed to reach the locally installed NATFW NSLP daemon.

8 SCTP and NSLP

NATFW NSLP can be useful for SCTP in two ways. It can reserve and open bindings on all NATs along the way on both sides and thereafter open the data flow from end to end. It can also tell the SCTP endpoint what public IP addresses are used on the edge NATs. For end-to-end NATFW NSLP signaling, it is necessary that each NAT along the path between the data sender and the data receiver implements the NSIS NATFW NSLP. We will discuss in this paper the most complex scenario that includes multi-point traversal on both sides. Solutions for other more simple scenarios can be derived from it.

8.1 Responding Endpoint Behind NAT

When the SCTP endpoints are located in different address realms and the responding endpoint (responder) is located behind a NAT, the initiating endpoint (initiator) cannot signal to the responder’s address directly. The responder is not reachable from the initiator using the private address of the responder and thus NATFW NSLP signaling messages cannot be sent to the responder's address.

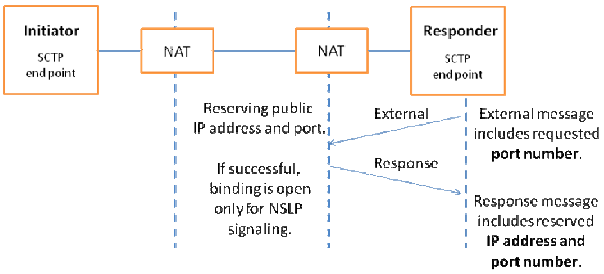
Initiator
SCTP end point
NAT
NAT
Responder
SCTP end point
Reserving public IP address and port.
If successful, binding is open only for NSLP signaling.
External
Response
External message includes requested port number.
Response message includes reserved IP address and port number.

Figure 8. Reservation of the port number using EXTERNAL message.

Slika 8. Rezervacija številke vrat z uporabo EXTERNAL sporočila

The responder acquires a public address by signaling on the reverse path (responder towards initiator) and thus making itself available to other hosts. This process of acquiring public addresses is called reservation. During this process the responder reserves publicly reachable addresses and ports suitable for further usage in SCTP association as shown in Figure 8. Reservation will only allow forwarding of signaling messages, but not data-flow packets.

Policy rules allowing forwarding of data flow packets set up by the prior EXTERNAL message signaling will be activated when the signaling CREATE message from initiator towards responder is confirmed with a positive RESPONSE message. A reservation made with EXTERNAL is kept alive as long as the responder refreshes the particular NATFW NSLP signaling session and it can be reused for multiple, different CREATE messages. In a multi-point traversal scenario the responder must reserve the same port number on all included NATs. If one or more NATs cannot reserve it, responder has an option to retry reserving a different port number on all NATs or it can exclude unsuccessful NATs from its source IP address list.

8.2 Initiating Endpoint Behind NAT

Initiator also has to know all public IP addresses of the included NATs on its side and reserve the same port number on them with EXTERNAL message as shown in Figure 9. If one or more NATs cannot reserve it, initiator has an option to retry reserving a different port number for all NATs or it can exclude unsuccessful NATs from its source IP address list.

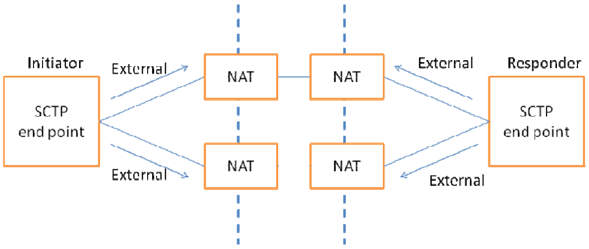

Figure 9. Reservations of a port number on all the included NATs on both sides.

Slika 9. Rezervacije številke vrat pri vseh vključenih NAT na obeh straneh.

After successful activation of NAT bindings and consequentially learning all public addresses, initiator starts sending CREATE messages as shown in Figure 10. For each used NAT a different CREATE message is sent to the distant SCTP endpoint public IP address, which can also mean the edge NAT on the other side. Every CREATE message must be sent via intended NAT. When the CREATE message is received at the public side of the NAT, it looks for a reservation made in advance, by using an EXTERNAL message. If there is a matching reservation, the NSLP stores the data sender's address (and if applicable the port number) as part of the source address of the policy rule (the remembered policy rule) to be loaded and forwards the message with the destination address set to the internal (private in most cases) address of responder. When the CREATE message is received at the private side, the NAT binding is allocated, but not activated.

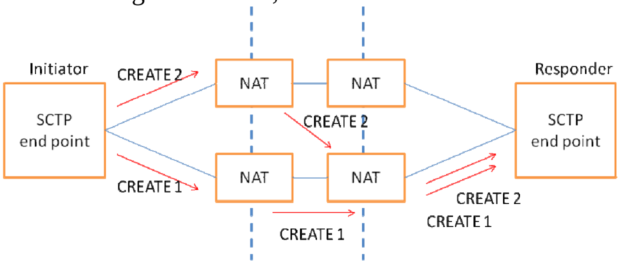

Figure 10. Opening of data flows using CREATE messages.

Slika 10. Odpiranje podatkovnih poti z uporabo CREATE sporočil.

After receiving RESPONSE messages for all sent CREATE messages, SCTP endpoint knows that data paths on all possible network paths are open on its side, and therefore sends a SCTP message with the INIT chunk that contains the list of its public IP addresses to the responder’s public IP address. Responder sends back INIT ACK chunk and gives the initiator its IP address list. The data flow is presented in Figure 11.

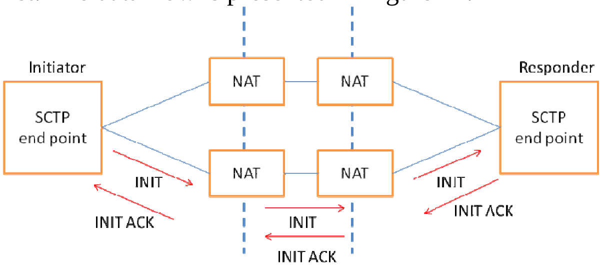

Figure 11. Initiation of SCTP association of one data path.

Slika 11. Vzpostavljanje SCTP povezave preko ene poti.

Initiator can continue the initiation of the SCTP association but cannot start sending heartbeat chunks to the IP addresses given in the list, with the exception of the source IP address in the IP header, or mark those paths active until it sends additional CREATE messages for every path and receives the appropriate RESPONSE messages as shown in Figure 12.

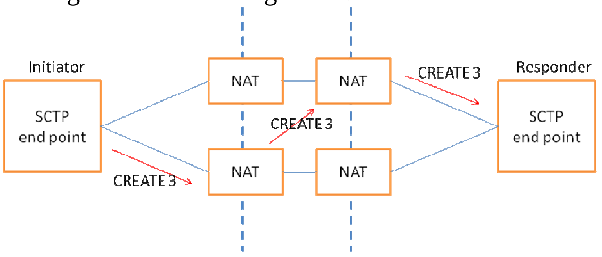

Figure 12. Opening of the remaining data flows using CREATE messages.

Slika 12. Odpiranje preostalih podatkovnih poti z uporabo CREATE sporočil.

9 Security Issues

Most security threats at the NATFW NSLP layer can be prevented by using a mutually authenticated Transport Layer Secured connection and by relying on authorization by the neighboring NATFW NSLP entities [3]. The NATFW NSLP relies on an established security association between neighboring peers to prevent unauthorized nodes to modify or delete the installed state. Between non-neighboring nodes the session ID (SID) carried in the NTLP is used to show ownership of a NATFW NSLP signaling session. The session ID is generated in a random way and thereby prevents an off-path adversary to mount targeted attacks. Hence, an adversary would have to learn the randomly generated session ID to perform an attack.

10 Conclusion

We explored the initialization of the SCTP association with NAT traversal. When using single-homed endpoints, solutions for NAT traversal are similar to those for TCP. For multi-homed endpoints traversal of more than one NAT is inevitable and a need arise to synchronize all the included NATs. One possible but unreliable solution is to count on the port preservation rule, where additional IP addresses can be added after SCTP endpoints are already associated. For other presented solutions we propose that SCTP endpoint acquires all the needed information about the included NATs before starting the initialization procedure and that those NATs are already configured to allow the traversal for the communication. NATs can be configured statically by an administrator or dynamically using some signaling protocol. We introduced the possibility of using NATFW NSLP for reserving the port number, acquiring public addresses and opening data flows over the included NATs. NSLP is transported with NTLP, which includes the usage of TSL for securing transport between the NSLP nodes. The owner of the NAT device can authenticate and decide which NSLP nodes can punch holes in NAT into its private realm.

Our proposed solutions can be used in many applications that find SCTP features useful for their purposes and have to communicate with users in private realms. Although applicability of NAT with IPv6 is questionable in future [12], the usage of NAT will not fade quickly. Further research will be based on implementing and testing our proposed solution. Research will be conducted using OpenNSIS [25] project implementation of the NTLP and NSLP protocols and adjust them, so that they will work in collaboration with SCTP open source implementation lksctp. The solution will enhance performance and usability of protocols that we work on in the Laboratory for telecommunication at the Faculty of Electrical Engineering of the University of Ljubljana. In our own implementations of SIGTRAN protocols and DIAMETER we use SCTP.

References

[1] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[2] Stewart, R., Xie, Q., Tuexen, M., Maruyama, S., and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC 5061, September 2007.

[3] M. Stiemerling, H. Tschofenig, C. Aoun, and E. Davies, “A NAT/Firewall NSIS signaling layer protocol (NSLP)”, Internet draft (draft-ietf-nsis-nslp-natfw-16), work in progress, November 2007.

[4] H. Schulzrinne, R. Hancock “GIST: General Internet Signalling Transport«, Internet draft (draft-ietf-nsis-ntlp-14), work in progress, July 2007.

[5] L. Coene, " Stream Control Transmission Protocol Applicability Statement", RFC 3257, April 2002.

[6] F. Audet, Ed., C. Jennings " Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", RFC 4787, January 2007.

[7] P. Srisuresh, Xie, K. Egevang, M, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[8] Ahmed Abd El Al, Tarek Saadawi, Myung Lee, "A Transport Layer Load Sharing Mechanism for Mobile Wireless Hosts", PERCOMW’04, March 2004.

[9] J. Rosenberg, R. Mahy, P. Matthews, D. Wing “Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)”, Internet draft (draft-ietf-behave-turn-05), work in progress, November 2007.

[10] M. Riegel, M. Tuexen, “Mobile SCTP«, Internet draft (draft-riegel-tuexen-mobile-sctp-07), work in progress, October 2006.

[11] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[12] Cisco Systems "The coming internet evolution: IPv6 and its implications for the service provider marketplace", white paper, 2004.

[13] C. Boulton, J. Rosenberg, G. Camarillo, “Best Current Practices for NAT Traversal for SIP«, Internet draft (draft-ietf-sipping-nat-scenarios-07), work in progress, July 2007.

[14] B. Carpenter, S. Brim, "Middleboxes: Taxonomy and Issues", RFC 3234, February 2002.

[15] J. Rosenberg, “Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer /

Answer Protocols «, Internet draft (draft-ietf-mmusic-ice-16), work in progress, June 2007.

[16] Shigeru Kashihara, Katsuyoshi Iida, Hiroyuki Koga, Youki Kadobayashi, Suguru Yamaguchi, “Multi-path Transmission Algorithm for End-to-End Seamless Handover across Heterogeneous Wireless Access Networks”, IEICE 2004: 490-496, March 2004.

[17] S.J. Koh, M.J. Chang, M. Lee, mSCTP for soft handover in transport layer, IEEE Communication Letters 8 (3) (2004) 189-191

[18] Li Ma, F. Yu, V. Leung, and T. Randhawa, “A New Method to Support UMTS/WLAN Vertical Handover Using SCTP” IEEE Vehicular Technology Conference, vol. 3, 2003, p. 1788--1792

[19] Natarajan, P., Iyengar, J.R., Amer, P.D., Stewart, R., “Concurrent Multipath Transfer using Transport Layer Multihoming: Performance Under Network Failures” Military Communications Conference, 2006. MILCOM 2006, Page(s):1 - 7

[20] C. Jennings, “NAT Classification Test Results«, Internet draft (draft-jennings-behave-test-results-04), work in progress, July 2007

[21] L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdrege, and C. Sharp, "Framework Architecture for Signaling Transport", RFC 2719, October 1999.

[22] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[23] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler "SIP: Session Initiation Protocol", RFC 3588, June 2002.

[24] J. Rosenberg, H. Schulzrinne, G. Camarillo "The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)", RFC 4168, October 2005.

[25] ”An Implementation of the Next Steps in Signaling (NSIS) Protocol Suite at the University of G¨ottingen”, http://user.informatik.uni-goettingen.de/˜nsis/.

The research was supported in part by the Ministry of Higher Education, Science and Technology of the Republic of Slovenia and in collaboration with Iskratel.

Tine Stegel received his B.S. degree in the field of Telecommunications from the Faculty of Electrical Engineering of the University of Ljubljana. He is currently employed with the same faculty working in the laboratory for Telecommunications. His research area includes transfer of SS7 signaling over IP and his project work deals with implementing and testing of the SIGTRAN protocols. His teaching activities are focused on areas about SIGTRAN and networking in Cisco Networking Academy Program.

Janez Sterle graduated in 2003 from the Faculty for Electrical Engineering, University of Ljubljana, where he is currently working towards a post-graduate degree. Since 2002 he has been working in the Laboratory for Telecommunications. His educational, research and development work is oriented towards design and development of next generation networks and services. His current research areas include multiprotocol label switching, next generation internet protocol, network security and development and deployment of new integrated services into fixed and wireless access networks. Since 2003 he has been actively working in the Cisco Networking Academy program at the Faculty for Electrical Engineering.

Andrej Kos received his B.Sc. and Ph.D. degrees from the Faculty of Electrical Engineering of the University of Ljubljana, Slovenia, in 1996 and 2003, respectively. His work interest is in analysis, design and development of telecommunications systems and services, fixed and mobile networks, service platforms and protocols. He is a member of IEEE, IEICE and Telemanagement Forum.

Janez Bešter received his Ph.D. degree in the field of telecommunications from the University of Ljubljana, Slovenia. He is currently the Head of the Laboratory for Telecommunications and is an Associate Professor at the Faculty of Electrical Engineering in Ljubljana. His work focuses on planning, realization and management of telecommunication systems and services as well as applying information and communication technologies to education.