An NSIS-based Approach for Firewall Traversal in Mobile IPv6 Networks

Niklas Steinleitner, Xiaoming Fu,
Dieter Hogrefe
University of Göttingen
Göttingen, Germany
{steinleitner,fu,hogrefe}
@cs.uni-goettingen.de

Thomas Schreck, Hannes Tschofenig
Nokia Siemens Network AG
Munich, Germany
thomas.schreck@fh-landshut.de
tschofenig@nsn.com

ABSTRACT

Firewalls have been successfully deployed in today's network infrastructure in various environments and will also be used in IPv6 networks. However, most of the current firewalls do not support Mobile IPv6, the best known solution for mobility support in IPv6. As a result, Mobile IPv6 traffic will be most likely dropped without appropriate firewall traversal solution.

This paper describes the problems and impacts of having firewalls in Mobile IPv6 environments and presents a firewall traversal solution based on the IETF's Next Steps In Signaling (NSIS) framework to address these issues. Compared with other candidates such as STUN, TURN, ICE, ALG, MIDCOM and COPS, this approach does not rely on specific firewall placements and can be applied in various operational modes without introducing a third entity. Authentication aspects are also explored.

1. INTRODUCTION

Middleboxes such as firewalls are an important aspect for a majority of IP networks today. Current IP networks are predominantly based on IPv4 technology, and hence various firewalls (as well as Network Address Translators(NATs)) have been originally designed for these networks. Deployment of IPv6 networks is currently work in progress. However, some firewall products for IPv6 networks have already been developed. It is foreseen that firewalls will become an indispensable means for protecting against unwanted traffic in operational IPv6 networks especially in enterprise environments.

Given the fact that Mobile IPv6 [1] is a recent standard, most firewalls available for IPv6 networks still do not support Mobile IPv6. Unless firewalls are aware of Mobile IPv6 protocol details, they will have to either block Mobile IPv6 communication traffic, or carefully deal with the traffic by per-user or per-connection, or allow this traffic in general through manual pre-configuration. This could be a major impediment to the successful deployment of Mobile IPv6.

Some existing firewall traversal protocols, such as STUN [2], TURN [3], ICE [4], Application Layer Gateways, Middlebox Communication [5], COPS [6], SNMP or policy-based solutions potentially can be extended for performing firewall and middlebox traversal even in mobile networks. However, some of them require prior knowledge of the existence of firewalls and most do not address the issue of discovering firewalls. Furthermore, they do not support the node mobility case and thus may require significant efforts to be extended for use in Mobile IPv6 networks.

A recent initiative within the IETF, Next Steps in Signaling (NSIS) [7], has developed a signaling protocol for firewall and NAT traversal. NSIS utilizes a two-layer signaling paradigm, which defines a lower layer for general extensible IP signaling and a layer for various signaling applications such as signaling for NAT/Firewall traversal. Since its initial design, NSIS has been considering node mobility as its potential use scenarios, and the mobility support for the NSIS framework is being discussed in [8]. However, how the NSIS firewall/NAT traversal signaling protocol supports IPv6 mobility is not specified.

This paper will give an overview of the problems when firewalls are placed in Mobile IPv6 networks, identify potential approaches and present how one can use NSIS to address the Mobile IPv6 firewall traversal issues.

The paper is structured as follows. In section 2 we shortly describe the problems and impacts of having firewalls in Mobile IPv6 environments as described in RFC4487 [9] and identify potential state-of-the-art solutions. In section 3 we present a middlebox traversal solution based on the NSIS signaling layer protocol for NAT/firewall traversal (NAT/FW NSLP) [10] and show how it can be used for firewall traversal in Mobile IPv6. Section 4 provides an analysis of potential authorization solutions and section 5 discusses open issues and further work. Section 6 summaries this paper.

2. PROBLEM STATEMENT

To study how firewall traversal can be achieved in Mobile IPv6 environments, it is necessary to understand the problems and impacts of having firewalls in such environments.

Mobile IPv6 [1, 11] introduces several new types of messages, which can be categorized into registration messages (Binding Update(BU), Binding Acknowledgements(BA)), Home/Care-of-testing messages (Home-of-Test-Init (HoTI), Home-of-Test (HoT), Care-of-Test-Init (CoTI), Care-of-Test (CoT)) and data messages. A new mobility header is introduced in all this new messages, and all messages between the mobile node (MN) and the home agent (HA) are IPsec ESP [11] encapsulated.

When a user moves to a visited network, a firewall – no matter it is located in the home network, the visited network or the access network of the corresponding node – will affect the Mobile IPv6 signaling and data messages. For instance, route optimization, an integral part of Mobile IPv6 specification, does not work with the state-of-the-art firewalls that utilize stateful packet filtering (SPF). This set of extensions is a fundamental part of the protocol, enabling optimized routing of packets between a mobile node and its correspondent node, thus providing optimized communication performance. However, firewall technologies do not support Mobile IPv6 or are not even aware of IPv6 mobility extension headers. Since most networks in the current business environment deploy firewalls, this may prevent future large-scale deployment of Mobile IPv6. Secondly, another mode of communication in Mobile IPv6, namely bi-directional tunneling, does not work under some scenarios, e.g., when a firewall is placed in the access network or the home network. In addition, it is difficult for the Mobile IPv6 binding update packets (encapsulated using IPsec ESP) to traverse firewalls. In summary, these deployment issues with firewalls occur due to the nature that the commonly used firewalls posseses [9]:

- do not understand Mobile IPv6 mobility header,
- do not allow IPsec – which is used for Mobile IPv6 registration messages between MN and HA – traffic to traverse,
- do not understand data packets encapsulated in Mobile IPv6 and likely drop them.

In the following subsections, we first explore these problems in detail from both operational and technical aspects regarding some relevant scenarios.

2.1 Scenarios and issues

Without loss of generality, let us consider a typical roaming scenario, where a mobile user with a PDA (MN) is roaming outside of his company (hereafter, the so-called "Mobile Service Provider", or MSP) into a visited network ("Access Service Provider", or ASP) which is also a corporate network. The MN wants to communicate with his home network or its HA (in order to register its new location) and additionally with another node, the corresponding node (CN), for data communication. The visited network could be protected by a firewall, thus parts of the traffic to the MN may be blocked. Besides, both the home network and the network of the CN may deploy firewalls. These three possible firewall placements introduce several problems, which could prevent Mobile IPv6 from operating successfully in the presence of firewalls. In all cases, pinholes have to be open on the firewalls for enabling successful communication. These problems can be differentiated under three basic scenarios.

- Firewall located at the edge of the MN's ASP,
- Firewall located at the edge of the CN's ASP,
- Firewall located at the edge of the MN's MSP.

In the following sections we investigate these three basic scenarios individually, and show how a firewall might prevent Mobile IPv6 from a successful operation.

2.1.1 *Firewall located at the edge of MN's ASP*

The first scenario assumes that the MN roaming to another network (i.e., ASP, which deploys a firewall (ASP-FW)) wants to enjoy communication with his home/company/ISP (MSA/MSP/ASA). Therefore, the MN needs to traverse the ASP-FW.

Figure 1 depicts how the components are placed in this scenario. Several issues need to be considered:

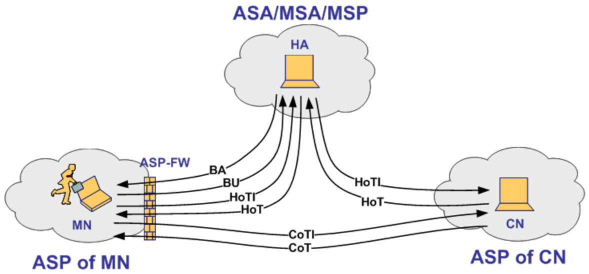

Figure 1: Firewall located at the edge of MN's ASP

- Both Binding Updates and Binding Acknowledgements, should be protected by IPsec ESP, but many firewalls drop IPsec ESP packets because they cannot determine whether inbound ESP packets are authorized. A possible solution might be to manually pre-configure the ASP-FW so that MIPv6 traffic are allowed to traverse it. However, not every administrator would permit IPsec traffic in general, so it must also be possible to dynamically install this firewall rules.
- The ASP-FW may drop the Home Test messages and prevent the completion of the Return Routability Test (RRT) procedure, as the Home Test messages of the RRT are protected by IPsec ESP in the tunnel mode. Therefore, either manual pre-configuration or dynamic on-demand configuration of rules on the ASP-FW is a possible solution for this type of messages.
- If the MN successfully sends a Binding Update to it's HA and the subsequent traffic is sent from HA to MN (in bi-directional tunneling), there is also no corresponding state on the firewalls, and the firewalls drops the incoming packets. Hence, it is necessary to dynamically configure the ASP-FW to let this data traffic traverse.
- The ASP-FW may prevent correspondent nodes from establishing communications (e.g. route optimization traffic) because incoming packets are dropped since the packets do not match any existing state.
- If the MN roams and moves to another access network protected by a different firewall, all new incoming packets are dropped as they do not match any existing "allow" state.

2.1.2 *Firewall located at the edge of CN's ASP*

Here, an MN visiting another company (i.e., MN-ASP) outside his company/ISP wants to communicate with his home network and a network (CN-ASP) which deploys a firewall.

Therefore, the traffic from the MN to the CN (transmitted with bi-directional tunneling or route optimization) needs to traverse the CN's ASP-FW.

Figure 2 depicts how the components are placed in the second scenario. Several issues need to be considered:

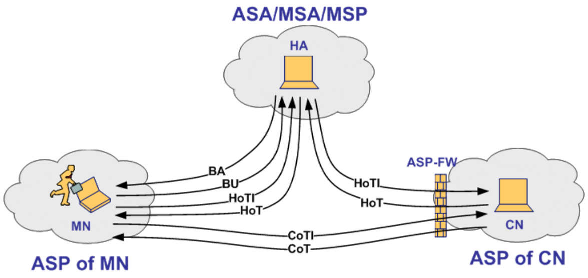

Figure 2: Firewall located at the edge of CN's ASP

- The Care-of-Test-Init message is sent using the Care-of-Address (CoA) of the MN as the source address. Such a packet does not match any entry in the protecting firewall, as the states in the firewall are bounded to the old address of the MN. The CoTI message will thus be dropped by that firewall. As a consequence, the RRT cannot be completed, and route optimization cannot be performed. Every packet has to go through the HA and be tunneled between the HA and the MN.
- If the BU to the CN is successful, the firewall still drops packets that are coming from the CoA, because these incoming packets are sent from the CoA and do not match any existing firewall state.

2.1.3 Firewall located at the edge of MN's MSP

In this scenario, the MN roaming to another company/ISP (i.e., ASP) wants to enjoy communicating with a CN and his own company (MSP), and the MSP deploys a firewall at its network border. The MN needs to traverse the MSP-FW to run Mobile IPv6.

Figure 3 depicts how the components are placed in third scenario. Several issues need to be considered:

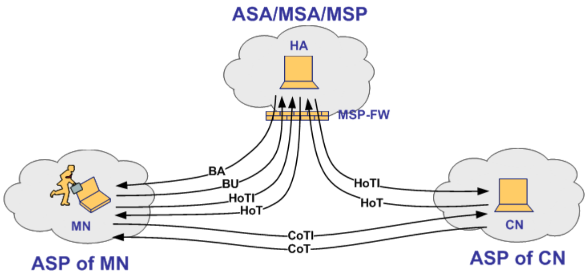

Figure 3: Firewall located at the edge of MN's MSP

- If the firewall protects the home agent by blocking ESP traffic, some of the MIPv6 signaling (e.g., Binding Update, HoTI) may be dropped at the firewall. This prevents MNs from updating their binding cache and performing Route Optimization, since the messages must be protected by IPsec ESP. Manual pre- configuration is a solution, but also has some problems as mentioned before.
- If the firewall is a stateful packet filter and protects the home agent from unsolicited incoming traffic, the firewall may drop connection setup requests from CNs, and packets from MNs.

2.2 Mobile IPv6 Firewall Traversal, Requirements and Solution Alternatives

To get Mobile IPv6 work in this scenarios it is necessary to allow all this messages to traverse the firewall. This requires the usage of a middlebox configuration solution. In general we can distinguish between two types of middlebox configuration; the implicit and the explicit approaches. The implicit middlebox configuration is triggered by data traffic. Here it is assumed that all middleboxes between the sender and the receiver behave well, otherwise such an implicit approach is not supported on a path. Several implicit approaches have been proposed, e.g. STUN, TURN and ICE. In contrast, the explicit middlebox configuration is typically triggered by signaling traffic. All these approaches, such as Application Layer Gateways, Middlebox Communication or the NAT/Firewall NSLP, can rely on an open and standardized protocol behavior.

The additional signaling within the explicit middlebox configuration solutions represents on the one hand the most important disadvantage, as it requires at least one additional round trip to signal for the necessary pinholes. The implicit approaches do not require any additional signaling. On the other hand, this signaling also represents the biggest advantage of this approaches, as it allows a more flexible pinhole creation. Implicit approaches can only be used for normal kind of data traffic, defined by a 5-tuple. In contrast, explicit approaches can signal for very fine pinholes, e.g. IPsec SPI, type of headers (e.g. Mobility, Destination or Routing Header) or even the fields of this headers. Due to this and to the fact that implicit approaches might not work in some scenarios, as they rely on the behaviour of all involved nodes, explicit approaches are preferable for Mobile IPv6 firewall traversal.

Application Layer Gateways

Application Layer Gateways relies on the installation of a enhanced Firewall/NAT, called an ALG. This ALG is aware of the protocol details and "understands" the signaling messages and their context within the protocol. The ALG processes the signaling and media messages and can modify the signaling to match the public IP addresses and ports which are used by the signaling and media traffic. The ALG is transparent to end hosts and does not terminate sessions with either end host. Instead it interacts with a middlebox to set up middlebox state, access control filters, use middlebox state information, modify application specific payload, or perform whatever else is necessary to enable the application traffic to run through the middlebox. The complexity of ALG depends on the application level knowledge required to process payload and maintain state. Ideally, the ALG should be simple and not require excessive computation or state storage. Depending on the protocol, an ALG may be difficult or easy to construct, though in some cases it may not be possible at all. When encrypted by end-to-end ESP, such payloads are opaque to application layer gateways. In this case, ALG will not help much. The

ALG-technique requires replacement of the existing firewall with an ALG. Alternatively, some vendors provide software upgrades to their firewalls to support ALG functionality. However, when several middleboxes exist in the path, each one of them needs to be updated to support new protocols - like Mobile IPv6. Another issue is that the ALG performance may become the bottleneck of the middlebox.

STUN/TURN/ICE

One alternative is the Interactive Connectivity Establishment (ICE) which is defined in [4]. ICE is not a new protocol, it is a framework which uses STUN and TURN to establish a connection to the remote pair. It is mainly designed for NATs but could be used for firewall traversal as well. STUN provides a client to discover whether it is behind a NAT, the NAT's typ and identify it's public IP address and port. The client sends a STUN request message to the STUN server, which is located in a public address space. The STUN server now knows the clients public IP address and port and will inform the client. For now on the client could use this information to receive data on this address and port.

The disadvantage of STUN is that it would not work with symmetric NATs and with incoming traffic. So ICE uses TURN which solves this problems. TURN allows a client behind a NAT to receive incoming data in this way, that a TURN server in the Internet will relay this traffic from the external IP address and port to the client. The client has to send packets through the TURN server to that address before, otherwise TURN would not know to which client this data traffic belongs.

ICE uses STUN and TURN to learn about the client's network topology. With this information the client could handle the problem to communicate through NATs and firewalls. But there are several disadvantages that come along with ICE. The first thing is that ICE is a really complex architecture. Further it was designed for NATs and so it does not guarantee that pinholes for MIPv6 traffic will be opened. There is also no support for mobility and so there is the need to customize ICE with the parameters needed for MIPv6 through firewalls. Another disadvantage of ICE instead of explicit solutions is that ICE does not provide any authorization mechanism which would be needed to verify if the client has the rights to communicate through a firewall with other nodes. ICE further needs some infrastructure, a TURN server and a STUN server which has to be located in the public Internet.

3. MOBILE IPV6 FIREWALL TRAVERSAL BASED ON NSIS

This section describes how an extended NSIS [7] NAT/FW NSLP [10] could be utilized to compose the Mobile IPv6 firewall pinhole creation. This approach has the advantage of being a modular IETF standard protocol able to configure stateful packet filters. One particular advantage is that the NSIS NAT/FW NSLP framework relies on a soft-state approach. Therefore, established sessions will be automatically torn down after a specified timeout. A soft state approach is very useful in a mobile scenario as it is not necessary to delete a session after roaming to another network. The University of Göttingen has developed an open source implementation of NSIS protocol stack [12], including a NAT/FW NSLP implementation, which allows customized extensions for development. The following section gives an overview of the NSIS Framework and the NAT/Firewall NSLP Framework, which have been developed by the IETF NSIS Working Group. It also describes how NSIS and the NAT/FW NSLP is applicable for Mobile IPv6 firewall traversal.

3.1 NSIS Introduction

The NSIS framework [7] has been developed with the goal of supporting various signaling applications, which install and manipulate certain control states in the network. Such states are meaningful for data flows and are installed and manipulated on network nodes supporting NSIS (NSIS Entities, NEs) along the data path. Not every node has to be such an NE, for instance, in the the NAT/FW NSLP case only NAT/Firewall boxes need to be the NEs along the data path of a data flow besides the end hosts. The basic protocol concept does not depend on any signaling application. This section describes the fundamental entities involved in NSIS signaling and their basic interactions. Two NSIS entities that communicate directly are said to be in a "peer relationship". This concept is also called as an NSIS hop. Such an NSIS hop must not be a single hop, i.e., an NSIS hop can accord with more real hops. Thereby, either or both NEs can store state information about the other NE, but it is not necessary to establish a long-term signaling connection between them.

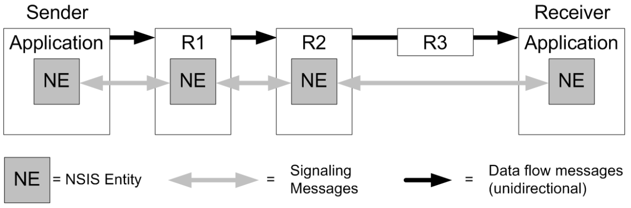

Figure 4: Simple Signaling and Data Flow Example

Figure 4 shows one of the simplest possible signaling configurations. A data flow is flowing from the sender via different routers to the receiver. The two end hosts and two of the routers contain NEs that exchange signaling messages about the flow. R3 does not contain an NE and forwards only the data. The signaling messages exchange is possible in both directions. Before a data flow is sent, an NSIS signaling procedure will take place along the NEs in the data path, including discovering their existence and signaling the application-specific states (e.g., firewall configurations for corresponding data traversal).

3.2 NSIS Layered Model Overview

In order to meet the modular requirements for NSIS, the NSIS protocol is structured in two layers:

- The NSIS Transport Layer Protocol (NTLP), which is responsible for moving signaling messages around and nevertheless independent from the underlying signaling application. The NTLP is implemented by GIST [12].
- The NSIS Signaling Layer Protocol (NSLP), which allows application based functionalities, such as message formats and sequences. Figure 5 illustrates this mod-

ular NSIS approach and the mutual influence between the NTLP and the NSLP.

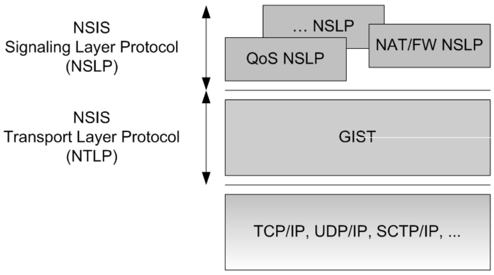

Figure 5: The NSIS Protocol Components

Functionality within the NTLP should be restricted only for transport and lower-layer operations. Other operations should be relocated to the signaling application layer. A short introduction of the NTLP can be described as follows. When an NSLP signaling message needs to be sent, the NSLP gives it over to the NTLP together with the information to which flow it belongs (so-called flow identifier). The NTLP has to care about how the message is sent to the next NE along the path and the NTLP is also working at the end of the path. The important advantage for the NTLP is the point that the NTLP do not need to have any knowledge about addresses, capabilities, or status of any NEs along the path, only for the NEs which it directly peers with.

Upon receipt of an NSIS message, each intermediate NTLP either directly forwards it or - if the signaling application runs locally - passes the message to the NSLP for further processing. After processing, the NSLP can use the original message or generate another message and hands it over to the NTLP. With this procedure end-to-end NSIS message delivery can be achieved. This restriction of the NTLP to peer-relationship scope simplifies the management and the complexity of the NTLP, at the cost of an increased functionality, complexity of the NSLPs and deployment complexity, as some components (e.g., middleboxes) on the path need to run NSIS.

3.3 The NAT/FW NSLP Protocol

The IETF NSIS working group is currently finalizing the NAT/Firewall NSIS Signaling Layer protocol (NAT/FW NSLP) specification [10], which describes scenarios, problems and solutions for path-coupled network address translator and firewall signaling. The NAT/FW NSLP is one of the two NSLPs that the working group has been developing. Our previous work [13] has shown that NSIS and the NAT/FW NSLP framework is able to support firewall signaling for up to tens of thousands of flows in parallel even in a low-end environment; and the overall performance bottleneck was found to lie in the utilized firewall implementation, not on the signaling implementation.

The main goal of NSIS NAT/FW signaling is to enable communications between two endpoints across different networks in case of the existence of NATs and firewall middleboxes. Firstly, it is assumed that these middleboxes will be configured in such a way that NSIS NAT/FW signaling messages can traverse them. Then the NSIS NAT/FW NSLP protocol is used to dynamically install additional policy rules in all NAT/FW NSLP-aware middleboxes along the path. Firewalls will be configured to forward desired data packets according to the policy rules which are established by the NAT/FW NSLP signaling.

The signaling traffic of an application behind a middlebox must traverse all middleboxes along the data path to establish communication with a corresponding application on the other end host. To achieve middlebox traversal, the application triggers the local NSIS entity to signal along the data path. If the local NSIS entity supports NAT/FW NSLP signaling, the knowledge of these application is used to establish policy rules and NAT bindings in all middleboxes along the path, which allows the data to travel from the sender to the receiver. Clearly, it is necessary for intermediate middleboxes to support NAT/FW NSLP, but not necessary for other intermediate nodes to support NAT/FW NSLP or even NSIS.

Figure 6 shows a common topology for the use of NAT/FW NSLP. This network is separated into two distinct administrative domains, namely “Domain A” and “Domain B”.

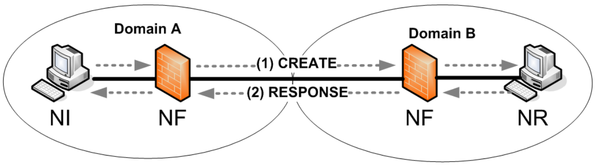

Figure 6: A Firewall Traversal Scenario

The NSLP Initiator (NI) sends NSIS NAT/FW NSLP signaling messages along the data path to the NSLP Responder (NR). It is assumed that NI, NR and every intermediate middlebox implements the NAT/FW NSLP. The signaling messages reach different intermediate NSIS nodes (i.e., NSLP Forwarder or NF) and every NAT/FW NSLP node processes the signaling messages and, if necessary, installs additional rules for the following data packets. The NAT/FW NSLP supports several types of signaling messages, most notably the CREATE and the EXT messages:

- The CREATE message is sent from the source address to the destination address and processed by every middlebox and forwarded to the destination.
- The EXT message is sent from the source address to an external address (e.g. the HA’s address or the CN’s address) and is intercepted by the edge firewall and not forwarded to the destination address. This allows signaling pinholes at the edge-firewall without introducing long end-to-end signaling delays.
- The RESPONSE message is used as a response to CREATE and EXT request messages.

Policy rules for firewalls are represented by a common 5-tuple, namely the source and destination addresses, the transport protocol and the source and destination port, in addition to the rule action with the value “allow” or “deny”. Such a policy rule in NAT/FW NSLP is bounded to a specified session. Different from other signaling applications where policy rules are carried in one object, the policy rules in NAT/FW NSLP are divided into an action (allow/deny), the flow identifier and further information. The message routing information (MRI) in the NTLP carries the filter specification, the additional information such as lifetime, session ID, message sequence number, authorization objects and the specified action are carried in NSLP's objects.

3.4 NSIS for Mobile IPv6 Firewall Traversal

As described in section 2, the standard Mobile IPv6 does not work with the existence of firewalls. To tackle these issues, one approach is to utilize a signaling protocol to install some firewall rules to allow these Mobile IPv6 messages to pass through. The NSIS NAT/FW NSLP, as described in [10], allows an end system to establish, maintain and delete middlebox state (i.e., firewall rules), and as well as allows packets to traverse these boxes. This protocol thus provides a possible way to address the aforementioned problems [14]. The following subsections introduce how we could extend the NSIS NAT/FW NSLP to solve the problems.

3.4.1 Firewall located in MN's ASP

In Figure 1, the MN is protected by a firewall that employs stateful packet filtering. The external CN and the HA are also shown in the figure. The MN is located in a visited network and is expecting to communicate with the CN. If the MN initiated normal data traffic there is no problem with the SPF firewall, as the communication is initiated from internal. The following subsections explain how this approach manages the MIPv6 signaling traffic problems as described in section 2.

Binding updates

IPsec protected binding updates cause problems in some deployment environments, as described in RFC4487 [9]. As a solution, NAT/FW NSLP can be used to dynamically configure the firewall(s) to allow the IPsec packets and associated traffic like IKE/IKEv2 packets to traverse, before sending the binding updates. Therefore, IP Protocol ID 50 should be allowed in the filter policies in order to allow IPsec ESP and IP Protocol ID 51 to allow IPsec AH. The firewall should also allow IKE packets (to UDP port 500) to bypass, which can also be signaled before.

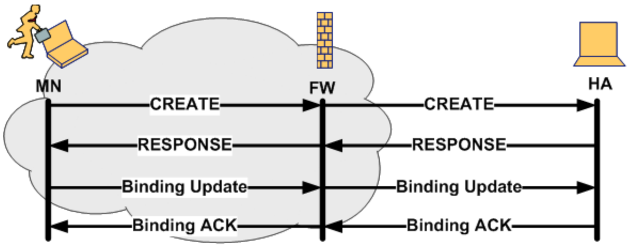

Figure 7: Signaling for BU and BA

Figure 7 shows the message flow for this signaling. As the firewall is a SPF, the subsequent binding acknowledgement from the HA to the CoA can pass the firewall, as it matches an existing state in the table.

Route optimization

Immediately after moving into a new network, the MN acquires a new CoA, performs the pinhole creation as described before and runs the Binding Update to the HA. The HoTI message from the MN is IPsec encapsulated in tunnel mode and as it does not belong to the session initiated by the MN or match a previously installed rule, it will be dropped by the firewall. Using CREATE, the MN initiates NSIS signaling to the firewall and open pinholes for the HoTI message. The message flow is comparable to the flow in Figure 7, whereas the CREATE message install different pinholes. The HoT message can re-use this pinhole and is able to reach the MN. The CoTI message and the CoT message can traverse the MN's ASP-firewall, as the CoTI message is not IPsec encapsulated and the CoT message correspond to the state previously installed by the CoTI message.

Once the RRT is successful, the binding update message is sent to the CN. If the MN wants to continue sending data traffic, no NSIS signaling is needed at all for this scenario. However, if the CN wants to send data traffic and the rules installed before matching again the addresses, the ports and the IPsec encapsulation, the relevant packet filter rules have to be installed at the firewall. If the rules installed before only matching again source and destination address, the data traffic exchanged with the CN in RO-case can also traverse the firewall with no need of installing additional rules. However, that would allow all kind of traffic from the CN and is rejected. Hence, the MN has to initiate sending data traffic to the CN but this happens after the RRT.

Bi-directional tunnelling

Consider the scenario where the MN is protected by a SPF. Even though the MN had earlier initiated a connection for the purpose of binding update, new filter rules have to be installed to allow the tunnelled data traffic as the rules before installed rules match again the addresses, the ports and the IPsec ESP encapsulation. The message flow is shown in Figure 8. If the MN is the data sender, no signaling is necessary at all. Otherwise, the MN opens pinholes to let the data messages traverse, with the help of EXT.

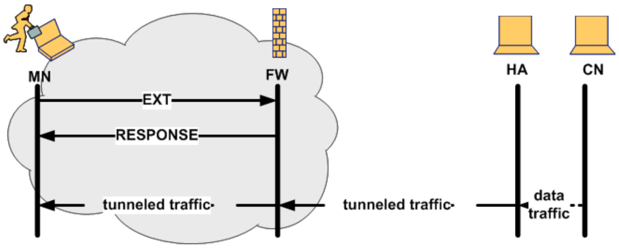

Figure 8: Signaling for data traffic

3.4.2 Firewall located in CN's ASP

Route Optimization

In Figure 2, the CN is protected by a firewall that employs the stateful packet filtering. The external MN and its associated HA are also shown in the figure. The MN communicates with the CN. If the CN initiated normal data traffic there is no problem with the SPF, as the communication is initiated from internal. The following subsections explain how this approach manages the MIPv6 signaling traffic problems as described in section 2.

The MN moves out of its home network and has to perform the return routability test before sending the binding update to the CN. It sends a HoTI message through the HA to the CN and expects a HoT message from the CN along the same path. It also sends a CoTI message directly to the CN and expects CoT message in the same path from the CN. The SPF will only allow packets that belong to an existing session and hence both the packets (HoTI, CoTI) will be dropped as these packets are Mobile IPv6 packets and these packets have a different header structure. The existing rules at the firewall might have been installed for some kind of data traffic. As the RRT procedure can not be executed, the firewall rules have to be modified to allow these MIPv6 messages to go through. The MN initiates the NSIS session by sending a CREATE message to the CN to install rules for the CoTI message. The NSIS signaling to allow the CoTI message is shown in Figure 9.

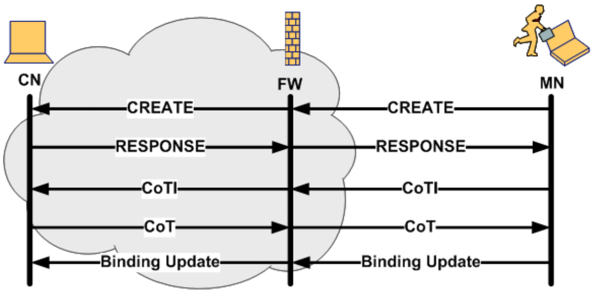

Figure 9: Signaling for CoTI and CoT

If the MN signal as described in the previous section, the HoTI is able to reach the HA. Nevertheless, the HoTI message from the HA to the CN is not able to traverse, as it does not match any state at the CN's ASP-FW. Therefore, either the HA or the CN has to signal install rules to let the HoTI traverse. When the MN receives both CoT and HoT messages, it performs binding update to the CN which is possible, as the BU can re-uses the previously installed rules. Note that the aforementioned signaling was only to allow the Mobile IPv6 messages.

If the CN wants to continue sending data traffic (CN is the data sender(DS)) to the new CoA, it can do so without any additional signaling. This is because the SPF will allow the traffic initiated by the nodes that it protects. But if the MN wants to continue sending data traffic (MN is the DS), it has to install filter rules for data traffic. The approach of combined signaling (for control and data traffic) could be useful, but currently the NSIS NAT/FW protocol does not support installing multiple rules at the same time. This will be discussed in section 5 in detail.

This solution works under the assumption that the firewalls will allow NSIS messages from external network to bypass, by applying a delayed packet filter state establishment and authorization from the CN. However, operators might be reluctant to allow NSIS message from external network as this might lead to Denial of Service (DoS) attacks. The CN might therefore be required to authorize the traversal of NSIS signaling message implicitly to reduce unwanted traffic. To avoid this complexity, it is also possible to ask the CN to open pinholes in the firewall on behalf of the MN. However, this solution may not work in some scenarios due to routing asymmetry as explained in [10].

Bi-directional Tunnelling

If the CN is protected by a SPF firewall, there is no need for any signaling if the CN starts sending data traffic. The CN sends the data traffic and hence the SPF will store relevant state information and accepts packets from the reverse direction.

If the HA is the DS, then either the CN has to initiate the signaling using EXT or the HA using CREATE, in order to configure the firewall to allow the data traffic traverse from the HA to CN. To support that function, Mobile IPv6 module at the HA or CN will need to be changed so that it triggers the local MIP6- firewall-traversal-application in the event of receiving a CoTI message from the MN. The local MIP6-firewall-traversal-application is then able to trigger the pinhole creation process. The message flow if the CN should signal for this pinhole is shown in Figure 10.

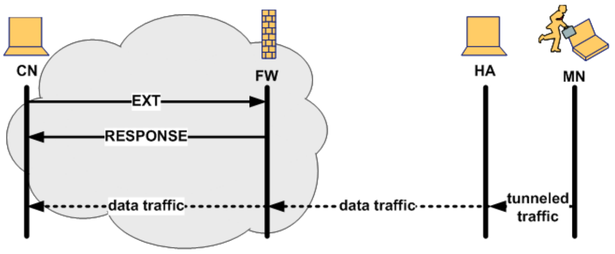

Figure 10: Signaling for data traffic

3.4.3 Firewall located at the edge of the MN's MSP

Route Optimization

In Figure 3, the Mobile Node's MSP is protected by a firewall that employs the stateful packet filtering. The MN and the CN are also shown in the figure. The MN, after entering a new network, sends a Binding Update to the HA. But as it is initiated by the MN, it first has to install some filter rules in the firewall before sending the Binding Update.

The MN-HA Binding Update message is assumed to be IPsec encapsulated. This might cause problems, as some primitive firewalls do not recognize IPsec traffic and hence drop the packets because of the absence of any transport header. One approach is to use UDP encapsulation of IPsec traffic in order to overcome this problem. Another is using NSIS NAT/FW NSLP to signal the firewall to allow such traffic to traverse. The MN initiates the NSIS signaling to create rules that will allow the Binding Update messages to go through the firewall. The MN then sends the Binding Update message to the HA.

By default, the rules previously installed in the firewall will not allow the HoTI message to go through. Hence, the MN has to install a different set of rules for these signaling messages by initiating another NAT/FW NSLP signaling exchange. After that it sends the HoTI message to the HA. The HA installs rules between the HA and the CN and accordingly send the HoTI to the CN. The HoT message from the CN to the HA is also allowed by the SPF as it belongs to the session previously installed by the HA. The HoT message from the HA to the MN is also allowed as it is initiated by the HA. The RRT completes successfully. Detailed message flow between MN and HA is shown in Figure 11.

For the data traffic, there is no additional signaling as the

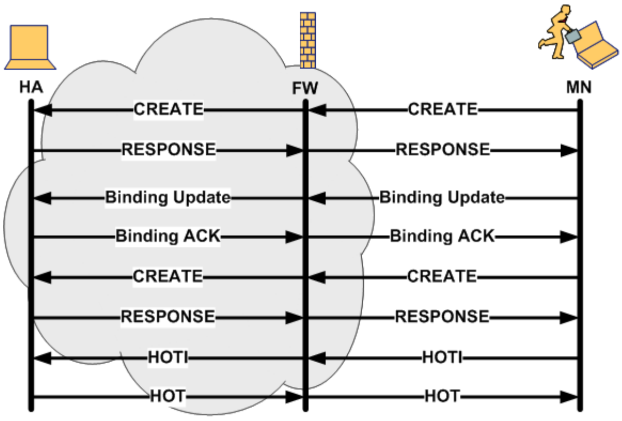

Figure 11: Signaling for BU, BA, HoTI and HoT

MN sends data directly to CN and none of these networks (CN network and MN network) are protected by firewalls. This is applicable for both cases when either MN or CN is the data senders.

Bi-directional tunnelling
Here, it is necessary that the HA opens pinholes for the data traffic from the CN using EXT. The CN is then allowed to send the data traffic through the firewall. After intercepting a packet, the HA tunnels it to the MN.

4. AUTHORIZATION AND KEY MANAGEMENT

An important issue is how to handle authorization for the signaling layer protocol. Manner et al. [15] specifies how authentication and authorization is implemented within the NSIS framework. The goal is to allow the exchange of information between nodes in order to authorize the usage of a resource. This is important for firewalls and MIPv6, as foreign networks do not know if the MN is allowed to communicate through it's firewall. Here we discuss three possible solutions to authenticate and authorize NAT/FW NSLP signaling, the Generic Service Authorization Architecture (GSABA) [16], an SAML and an EAP-TLS [17] approach.

4.1 Generic Service Authorization Architecture

The Generic Service Authorization Architecture (GSABA) [16] is an authentication system with three parties. The goal is to provide the end host the required information for serivce access based on credentials. In this section we will give an introduction to GSABA, show the architecture and later discuss a possible integration with NSIS NAT/FW NSLP in MIPv6.

4.1.1 GSABA Architecture

Figure 12 illustrates the basic architecture elements of GSABA. The Bootstrapping target (BT) is the entity that offers the requested service. In MIPv6 case, it is the firewall which will act as the BT. Another element in GSABA is the Bootstrapping Configuration Agent (BCA) which provides necessary bootstrapping information to the MN. The Bootstrapping Authorization Agent (BAA) will provide authorization statements based on the MN's profile. For roaming purposes there will be a new architectural element, the BAA Proxy. It's function is to forward the policies or to modify these policies.
One important interface between the elements is the Bootstrapping Target Protocol (TP-p) which provides the mechanism to exchange service related informations. RADIUS and Diameter are example protocols for TP-p. The Bootstrapping Protocol (BCA-p) will transmit bootstrapping information to the MN and also informs it about the authorization decision taken by the BAA and BAA Proxy. HTTP, SOAP and IKEv2 are possible candidates for the BCA-p interface. The protocols which delivers the decisions to the BCA and allows the exchange of necessary bootstrapping information, called the Bootstrapping Agent Protocol (BA-p), are also RADIUS and Diameter. The interface between the MN and the BT is the Service Related Protocol (SP).

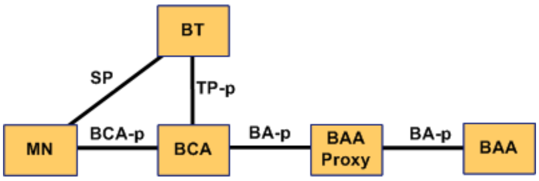

Figure 12: The GSABA Architecture

4.1.2 GSABA integration in NSIS NAT/FW NSLP

The integration of GSABA into the NSIS NAT/FW NSLP requires, in case of firewall traversal for Mobile IPv6, the investigation of the three scenarios:

- Firewall located at the edge of MN's ASP,
- Firewall located at the edge of CN's ASP and
- Firewall located at the edge of MN's MSP.

Here, the firewall acts as the BT and the GIST traffic is secured by TLS/PSK [18]. The NAT/FW NSLP Service Key is derived from the GSABA Key and the NAT/FW NSLP has to verify the authenticated identity. There are two elements, the GSABA Proxy and the GSABA Server. The GSABA Proxy consists of two network elements, the BCA and the BAA Proxy, the server is also a BCA and and BAA.

Firewall located at the edge of MN's ASP
When the MN wants to install rules at the firewall, it usually uses CREATE or EXT. Therefore, it has to be authorized against the GSABA Server before. Afterwards it will negotiate GSABA parameters with the GSABA Server over a protected EAP channel. When the MN was correctly authorized against the server, it will send the GSABA Key and it's user profile to the GSABA Proxy, which will store this information locally and informs the MN about the success. The MN gets the GSABA Key and is able to request HA information at the GSABA Proxy. The proxy checks whether the MN is authorized and selects a HA. After this the MN achieves its IKEv2 PSK and is able to authorize against the HA. The HA will fetch this PSK from the GSABA Proxy. When the MN is authorized, it derives the GIST Key and starts GIST TLS/PSK secured

handshake with the firewall. The firewall is able to fetch the PSK also from the GSABA Proxy.

Now, the MN could start the normal signaling; e.g. sending a CREATE message through the firewall to the local HA. The firewall checks the authorization after receiving the CREATE message. Figure 13 shows an example message flow how a MN will be authorized and installs firewall rules later on.

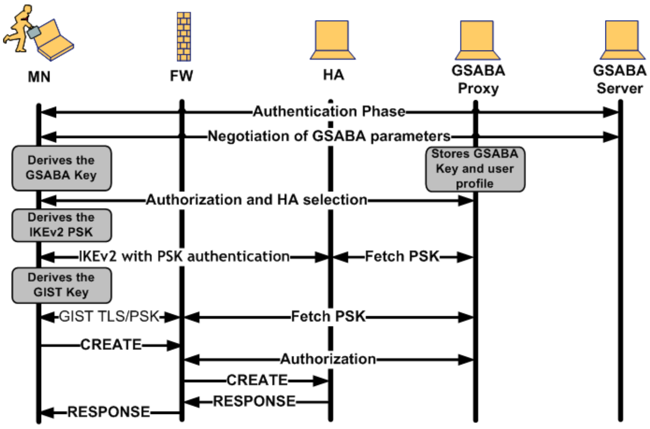

Figure 13: The GSABA message flow, Firewall located at the edge of MN's ASP.

Firewall located at the edge of CN's ASP

In this scenario, the CN needs to establish a security association between the firewall and itself. When the MN wants to open pinholes at this firewall, it firstly signals this with the CREATE message. As there is no authorization at this point, the firewall responses with a error message including it's domain name. The MN now derives a NSLP Key from the GSABA Key and sends the CREATE message again. At this time, the AUTH object will be included in the CREATE message. When the firewall receives this message, it fetches the NSLP Key from the GSABA Proxy which maybe need to get it from the GSABA Server. Hence, the firewall is able to authorize the message sent by the MN and forwards it to the CN, which replies with a RESPONSE message on the same path. The MN and the CN are now able to send the CoTI/CoT messages for route optimization. It is important to notice, that in this scenario the AUTH object is protected by an NSLP key which is bound to the domain name of the FW, not only to the firewall. This allows the signaling to traversal all firewalls within the CN's domain without deriving new keys for each firewall.

The message flow for the HoTI message is different as the MN sends the HoTI message including the AUTH object to it's HA which will then send the CREATE message, for opening pinholes, to the firewall. The firewall could now authorizes the CREATE message from the MN's HA. The later BU/BA messages between the MN and CN will later traverse the firewall with no problems.

Firewall located at the edge of MN's MSP

In this scenario, the MN first needs to be authorized against the GSABA Server to get the GSABA Key. Afterwards it generates the GIST Key out of the GSABA Key and start the GIST TLS/PSK Handshake. The firewall fetches the PSK and the MN could send a CREATE message to allow IKEv2 traffic to traverse the firewall. The firewall checks the authorization at the GSABA Server and then decides if the CREATE message can traverse the firewall. Afterwards, the MN derives IKEv2 PSK and authenticate using IKEv2 with that PSK against the HA. The HA could fetch the PSK from the GSABA Server. For further CREATE/RESPONSE messages, like BU, the MN is authorized against the firewall and the HA. Also if the HA uses the EXT message to install rules at the firewall, the HoTI/HoT message could easily be authorized.

4.2 SAML

SAML is an XML standard for exchanging authorization and authentication between two entities. A SAML Assertion is a packet of informations in which the Identity Provider lists all allowed operations.

A possible approach of applying SAML for NAT/FW NSLP signaling in Mobile IPv6 environments is proposed as follows. The MN first asks the Identity Provider to get such an assertion before to start signaling with the firewall. The Identity provider may need to ask the MN's MSP-AAA what credentials the MN has and afterwards will replay with this assertion. The MN can now install this SAML Assertion in the signaling message. After that the firewall verifies whether the assertion is valid and if the MN is authorized to open pinholes for further communication. If the firewall is not allowed to install the corresponding rules, it will inform the MN with an error message. Otherwise the normal signaling procedure starts and the MN is able to use Mobile IPv6. A disadvantage of using SAML is the huge overhead in the signaling message, because of using XML.

4.3 EAP-TLS

EAP-TLS [17] provides a flexible support for authentication and key exchange and is very easy to integrate with already existing AAA infrastructure like RADIUS and DIAMETER. When EAP-TLS is used, the MN needs to install its certificate in the NSIS authorization extension and indicates the availability of the EAP authentication mechanism. After the TLS handshake is finished, EAP will be used to authenticate with the exsting infrastructure. The advantage of using EAP-TLS would be that no additional components are needed and it would be integrated easily because NSIS already supports TLS as transport. A weakness of using EAP-TLS is the missing of specifying of credentials.

5. OPEN ISSUES AND FUTURE WORK

The firewall traversal solution based on IETF NSIS and the NAT/FW NSLP presented in this paper can deal with the problems of having firewalls in Mobile IPv6 environments. However, the approach as described might not be efficient enough, as the NAT/FW NSLP currently does not support the signaling of several pinholes within one message. As a result, the optimization and the reduction of the signaling delay will be of interest for further study. One approach is to extend the signaling protocol to allow signaling for multiple rules in one single message.

A firewall traversal approach like this needs a strong authentication and authorization framework. The initial authentication and authorization approaches in section 4 need to be

investigated in more detail.
Today's infrastructure mostly supports MIPv4, rarely MIPv6. Therefore, it is necessary to investigate a MIPv6 and MIPv4 Dual Stack solution as definied in [19].
We are currently finalizing a prototype implementation to prove the feasibility and the usability of such an Mobile IPv6 firewall traversal approach. As a next step, performance optimization and scalability aspects will be studied.

6. CONCLUSIONS

This paper shows how the NSIS NAT/FW NSLP can address the issues caused by stateful packet filter firewalls encountered in a Mobile IPv6 network. We described the problems and impacts of having firewalls in Mobile IPv6 environments and presented a firewall traversal solution based on the IETF NSIS framework, which can handle all these issues in the different scenarios. It has to be noted that a real scenario could include a combination of some set of these cases. In contrast to other middlebox configuration solutions, the NSIS solution does not have an issue with this. In any case, we assume that the MN, the CN, the HA and the firewalls are NSIS NAT/FW NSLP aware.
Compared with implicit middlebox configuration candidates, such as STUN, TURN, ICE, the NSIS approach can be applied without introducing an additional third entity. In contrast to the implicit approaches, all explicit approach like MIDCOM, COPS NAT/FW NSLP requires additional signaling. Instead, they are able to install finer firewall rules(e.g. for Mobility Header), which is necessary to get Mobile IPv6 traverse firewalls. Furthermore, the implicit approaches might fail in some scenarios, as they rely on the well behaviour of all involved nodes, but do not require that all involved nodes support the approach, as the explicit do. However, the performance of the explicit approaches often depends on the performance of the middlebox. This is not the case for the NAT/FW NSLP solution.
This paper shows that NSIS NAT/FW NSLP can address all the issues of having firewalls in Mobile IPv6 environments. Therefore, it represents a good potential solution and, to the best of our knowledge, currently the only one which addresses all issues. However, further study with respect for improvements as described in section 5 as well as the GSABA authorization interaction is necessary.

7. ACKNOWLEDGMENT

We would like to thank Ivano Guardini, Li Cai, Qin Wu, Ingo Juchem, Swen Weiland and Jan Demter for their contributions and insightful discussions.
This document is a by-product of the ENABLE Project, partially funded by the European Commission under its Sixth Framework Program. It is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ENABLE Project or the European Commission.

8. REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6 ", RFC 3775, June 2004.

[2] 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.

[3] J. Rosenberg, R. Mahy, C. Huitema, "Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN)", Internet draft (draft-ietf-behave-turn-02), work in progress, October 2006.

[4] J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", Internet draft (draft-ietf-mmusic-ice- 15), work in progress, March 2007.

[5] P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor, A. Rayhan, "Middlebox communication architecture and framework", RFC 3303, August 2002.

[6] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[7] R. Hancock, G. Karagiannis, J. Loughney, and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005.

[8] T. Sanda, X. Fu, S. Jeong, J. Manner, H. Tschofenig, "Applicability Statement of NSIS Protocols in Mobile Environments", Internet draft (draft-ietf-nsis-applicability-mobility-signaling-06), March 2007.

[9] F. Le, S. Faccin, B. Patil, and H. Tschofenig, "Mobile IPv6 and Firewalls: Problem Statement", RFC 4487, May 2006.

[10] M. Stiemerling, H. Tschofenig, and C. Aoun, "A NAT/Firewall NSIS signaling layer protocol (NSLP)", Internet draft (draft-ietf-nsis-nslp-natfw-14), work in progress, March 2007.

[11] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[12] "An Implementation of the Next Steps in Signaling (NSIS) Protocol Suite at the University of Göttingen", http://user.informatik.uni-goettingen.de/˜nsis/.

[13] N. Steinleitner, H. Peters, H. Tschofenig, X. Fu, "Implementation and Performance Study of a New NAT/Firewall Signaling Protocol", ADSN2006, in conjunction with ICDCS 2006, Lisboa, Portugal, IEEE, July 2006.

[14] S. Thiruvengadam, H. Tschofenig, F. Le, N. Steinleitner, X. Fu, "Mobile IPv6 - NSIS Interaction for Firewall traversal", Internet-Draft (draft-thiruvengadam-nsis-mip6-fw-06) work in progress, March 2007.

[15] J. Manner, M. Stiemerling, H. Tschofenig, "Authorization for NSIS Signaling Layer Protocols", Internet-Draft (draft-manner-nsis-nslp-auth- 03) work in progress, March 2007.

[16] F. Kohlmayer, H. Tschofenig, R. Falk, R. Lopez, S. Hernandez, P. Segura, A. Skarmeta, "GSABA: A Generic Service Authorization Architecture", MobiArch'06, San Francisco, December 2006.

[17] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[18] P. Eronen, H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)",

RFC 4279, December 2005.

[19] H. Soliman “Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)”, Internet draft (draft-ietf-mip6-nemo-v4traversal-04) work in progress, March 2007.