NSIS
Internet-Draft
Expires: May 19, 2008

N. Steinleitner, Ed.
X. Fu
Univ. Goettingen
F. Le
CMU
November 16, 2007

Mobile IPv6 - NSIS Interaction for Firewall traversal
draft-thiruvengadam-nsis-mip6-fw-08.txt

Status of this Memo

Copyright Notice

Abstract

Most of the firewalls deployed today are Mobile IPv6 unaware. Widespread Mobile IPv6 deployment is not possible unless Mobile IPv6 messages can pass through these firewalls. One approach is to use a signaling protocol to communicate with these firewalls and instruct them to bypass these Mobile IPv6 messages. The goal of this document is to describe the interaction between NSIS and Mobile IPv6 for enabling Mobile IPv6 traversal.

Table of Contents

1. Introduction

Route optimization, an integral part of Mobile IPv6 specification does not work with state of the art firewalls that employ stateful packet filtering (SPF). This problem is well described in [1]. The other mode of communication in Mobile IPv6, namely bi-directional tunneling, also do not work under some firewall placements. Apart from this, the Mobile IPv6 binding updates (encapsulated using IPsec ESP) packets also have problems with firewall traversal. To tackle these issues, one approach is to utilize a signaling protocol to install some firewall rules for allowing these Mobile IPv6 messages to pass through. The NSIS NAT/FW NSLP, as described in [2], allows to establish, maintain and delete middlebox state (i.e., NAT bindings and Firewall rules), and allow packets to traverse these boxes. This protocol thus provides a possible way to address the aforementioned problem. This document describe the considerations of NSIS NAT/FW NSLP, especially the involved messages and necessary firewall rules, when firewalls are encountered in a Mobile IPv6 network. More specifically, the following basic scenarios are studied individually.

- Mobile Node (MN) behind a firewall;
- Correspondent Node (CN) behind a firewall;
- Home Agent (HA) behind a firewall.

For every scenario, we will discuss how to apply NSIS signaling for the routing modes. It has to be noted that a real scenario could include a combination of some set of these cases. In any case, we assume that the MN, the CN, the HA and the Firewalls (FWs) are NSIS and NAT/FW NSLP aware. Also note that for every NSIS message, the underlying GIST[5] level provides flow-id information which will be used to install the firewall policies.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [3].

Furthermore, we use the same terminology as in [4], [2], and [6]. Apart from this, we use some abbreviations to describe the flow-id of the NSIS messages:

- SA-Source Address,
- DA-Destination Address,
- SP-Source Port,
- DP-Destination Port, and
- an asterisk is used as wild-card.

The term 'DS' refers to data sender and the term 'DR' to data receiver.

3. Mobile node behind a firewall

In Figure 1, the MN is protected by a firewall that employs stateful packet filtering (SPF). 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.

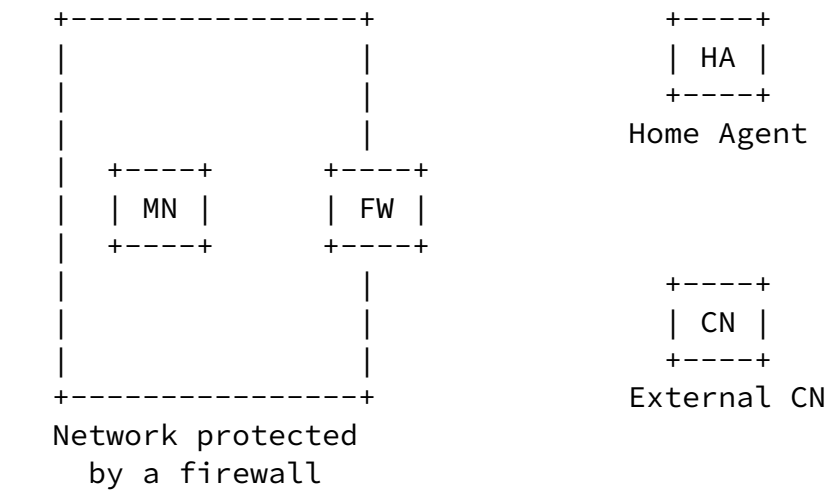


Figure 1: MN behind the firewall

3.1. Binding updates

IPsec protected Binding Updates cause problems in some deployment environments, as described in [1]. 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. 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 inside the firewall.

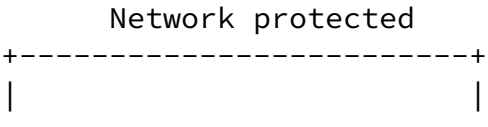
For the BU message (IPsec ESP in transport mode) from MN to HA, the MN installs rules using CREATE for the flow-id: SA: CoA, DA: HA, SPIx.

3.2. Route optimization

Immediately after moving into a new network, the MN acquires a new CoA, performs the pinhole creation as described in section Section 3.1 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 signalling to the firewall and open pinholes for the HoTI message. The message flow is shown in Figure 2. The HoT message can re-use this pinhole and is able to reach the MN.

For the HoTI message (IPsec ESP in tunnel mode) from MN to HA, the MN installs rules using the CREATE message for the flow-id: SA: CoA, DA:HA, SPIx.



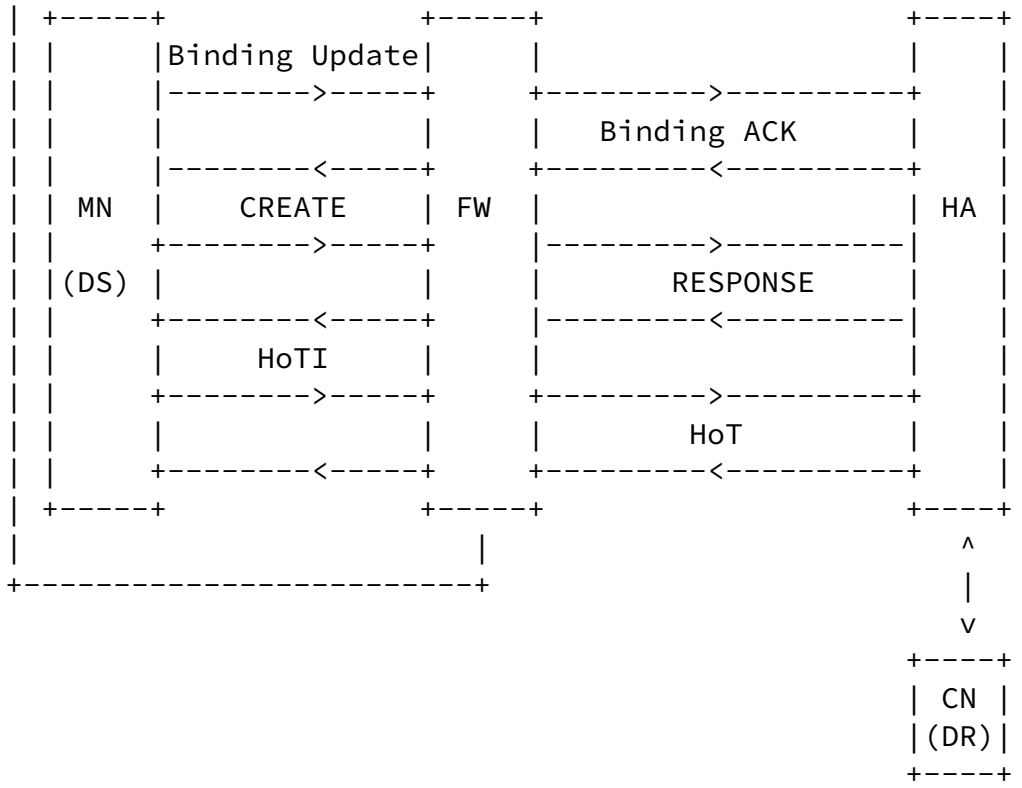


Figure 2: NSIS signaling for MN behind the firewall

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.

For the data traffic from CN to MN the MN installs rules using EXT for the flow-id: SA: CN, DA:CoA, SP: data application port, DP: data application port.

3.3. Bi-directional tunneling

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 3. If the MN is the DS, no signaling is needed at all. Otherwise, the MN open pinholes to let the data messages traverse, with the help of EXT.

For the data traffic from HA to MN, the MN installs rules using EXT for the flow-id: SA: HA, DA: CoA. Note these data messages for which we do signaling, are IP- in-IP tunneled messages.

Protected network

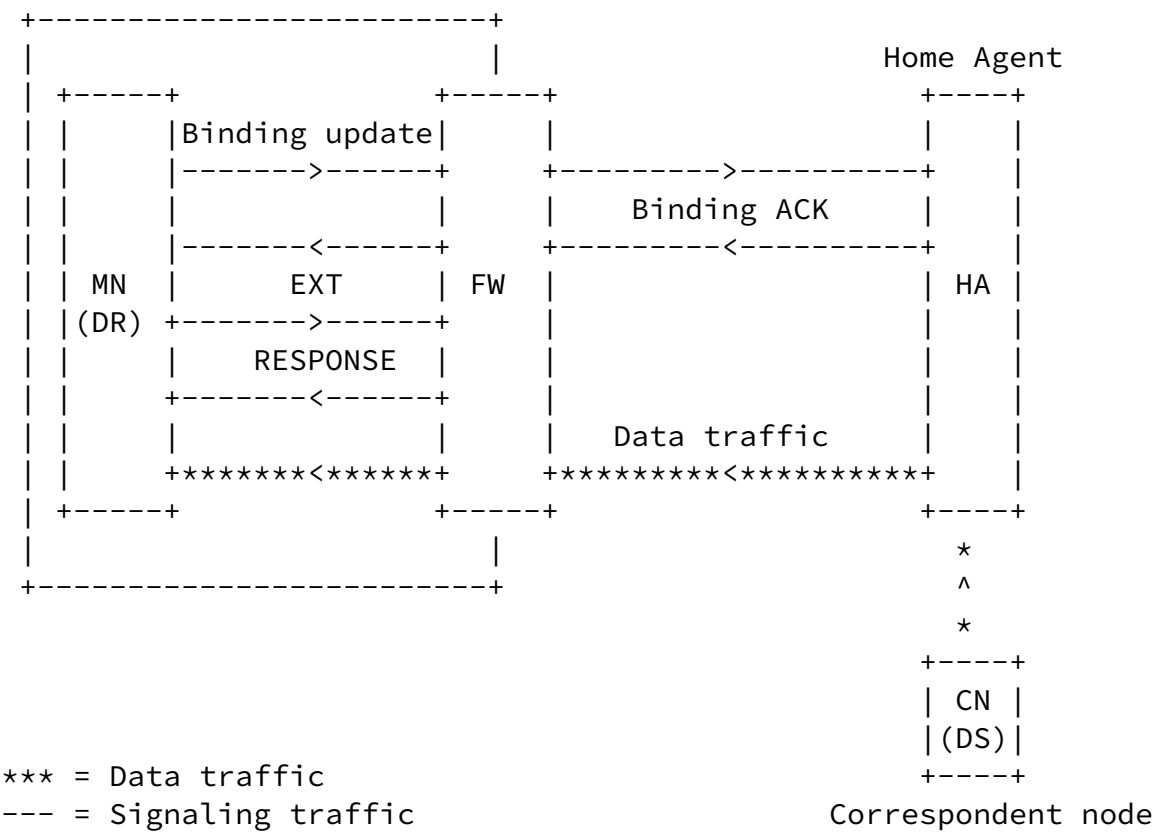


Figure 3: NSIS signaling for MN behind the firewall

3.4. Change of Firewalls

If the MN roams and attaches to a different firewall, the above-mentioned routing methods will have problems in traversing the new firewall. In this case the data sender (where it is MN or the CN or the HA) should re-signaling to the firewall using NSIS and establish the policies accordingly (mentioned above according to the routing methods).

Since the NAT/FW NSLP rely on a soft-state approach, established sessions will be automatically be teardown after a specified timeout value. Thus it is not necessary to delete or teardown a session after an MN roams to another network, as the protocol will do this by it own. More discussions about a possible alternative way by tearing down the established state are given in [7].

3.5. Operations when MN is behind a firewall

In summary, when a firewall is located in MN's ASP, the MN configures the firewall(s) using CREATE to let following messages traverse:

- Binding update messages (src: CoA, dst: HA, SPIx) (IPsec ESP in transport mode) {for BU}

- HoTI message (src: CoA, dst: HA, SPIx) (IPsec ESP in tunnel mode) {for RO}

MN configures the firewall(s) using EXT to let following traverse:

- for data traffic from HA to MN (src: HA, dst: CoA) {BT}

- for data traffic from CN to MN (src: CN, dst: CoA) {RO}

4. Correspondent Node behind a firewall

4.1. Route Optimization

In Figure 4, the CN is protected by a firewall that employs 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.

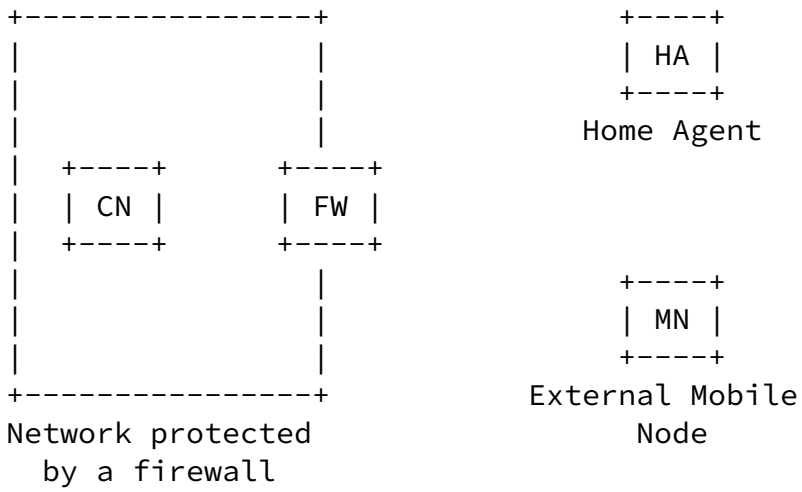


Figure 4: CN behind the firewall

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.

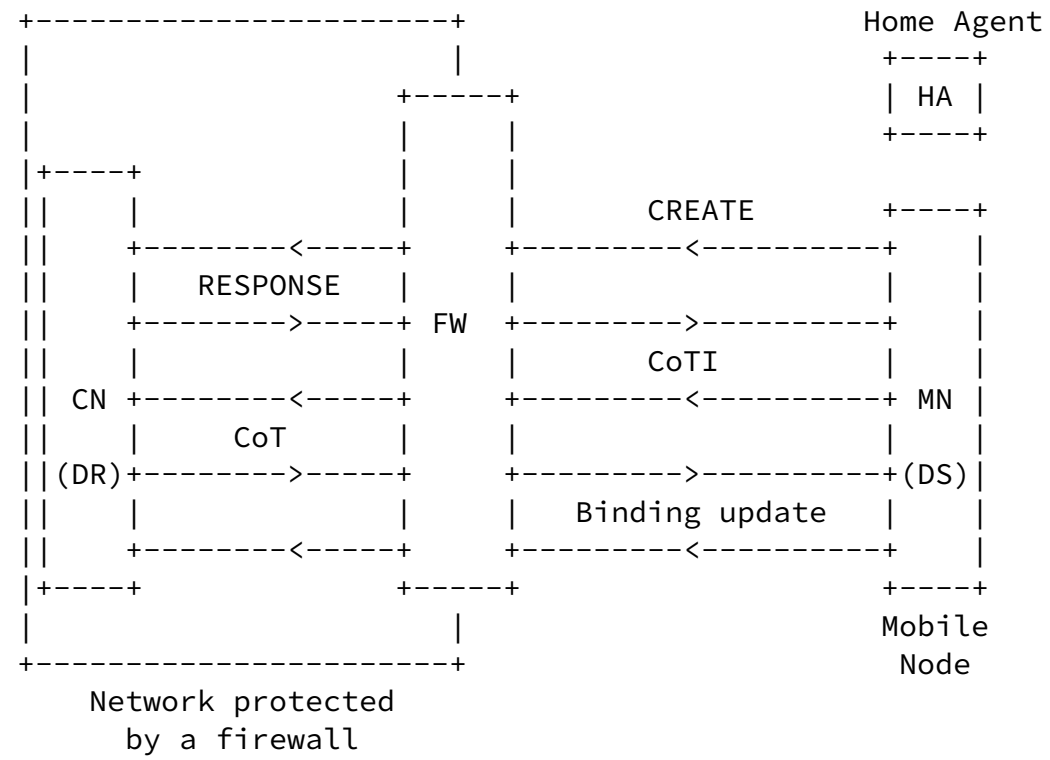


Figure 5: CN behind the firewall

As the RRT procedure cannot 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 5.

For the CoTI message from MN to CN, the MN installs rules using CREATE for the flow-id: SA: CoA, DA: CN.

This allows the CoTI to reach the CN. If the MN signal as described in section Section 3.2 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.

If the HA initiates the pinhole creation, the CREATE message for the HoTI message from HA to CN the flow-id will be: SA: HoA, DA: CN.

If the CN initiates the pinhole creation, the EXT message for the HoTI message from HA to CN the flow-id will be: SA: HoA, DA: CN.

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 signalling was only to allow the Mobile IPv6 messages.

If the CN wants to continue sending data traffic (CN is the 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 prospect 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.

For the data traffic from MN to CN, the MN installs rules using CREATE for the flow-id: SA: CoA, DA:CN, SP: data application port, DP: data application port.

This solution works with the assumption that the firewalls will allow NSIS messages from external network to bypass with 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 DoS attacks. The CN might therefore be required to authorize the traversal of NSIS signaling message implicitly to reduce unwanted traffic.

To avoid this, it is also possible to ask the CN to open pinholes in

the firewall on behalf of the MN. But this solution will not work in some scenarios due to routing asymmetry as explained in [2].

4.2. Bi-directional Tunneling

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.

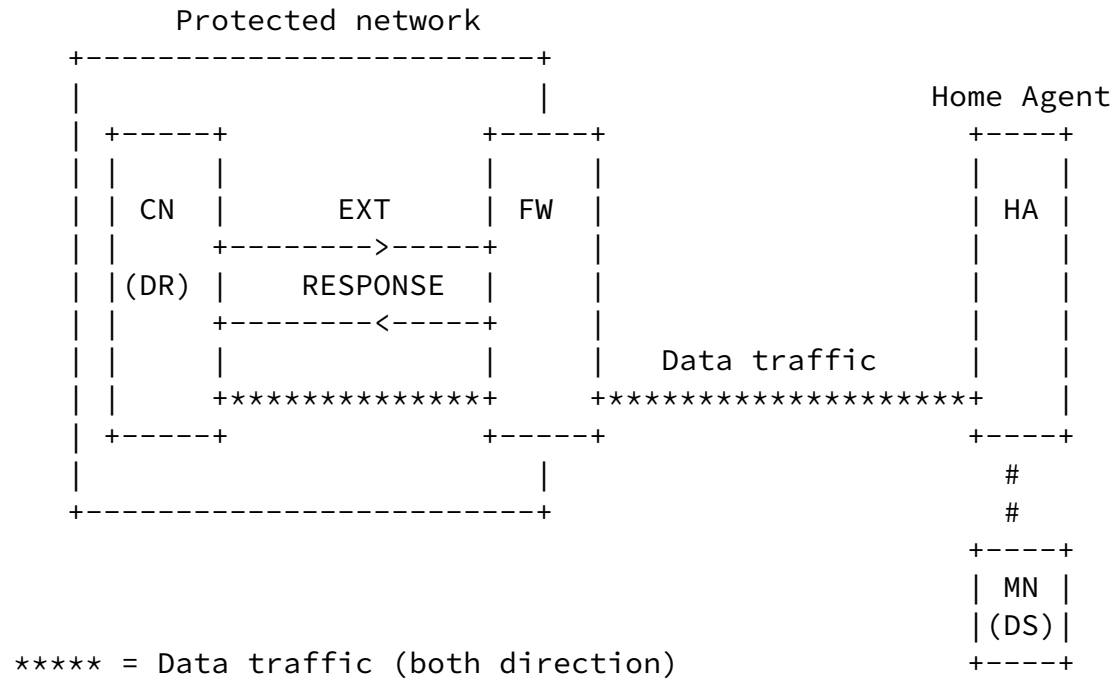


Figure 6: NSIS signaling for CN behind the firewall

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. The message flow if the CN should signal for this pinhole is shown in Figure 6.

If the CN initiates the pinhole creation, the EXT message for the data traffic from HA to CN the flow-id will be: SA: HA, DA: CN, SP: data application port, DP: data application port.

If the HA initiates the pinhole creation, the CREATE message for the data traffic from HA to CN the flow-id will be: SA: HA, DA: CN, SP: data application port, DP: data application port.

4.3. Change of Firewalls

If the MN roams and attaches to a network with a different firewall, the Mobile IPv6 protocol will be problematic again while traversing the newly encountered firewall, as the firewall is not configured appropriately. In this case the data sender (either the MN or the CN for both Mobile IPv6 signalling and data traffic, or the HA in case of Mobile IPv6 signaling traffic) should re-signal to the firewall using NSIS and establish the policies accordingly (following the similar procedures as described before). One possible enhancement would be to use the context transfer protocol between the old and new firewalls upon proper authorization of the operation; however this

approach will require further study.

4.4. Operations when CN is behind a firewall

In summary, when a firewall is located in the CN's ASP, MN configures the firewall(s) using CREATE to let following messages traverse:

- CoTI messages (src: CoA, dst: CN) {RO}
- for data traffic from MN to CN and vice versa (src: CoA, dst: CN) {for RO}

The HA configures the firewall(s) using CREATE to let following messages traverse:

- HoTI messages (src: HoA, dst: CN) {for RO}
- for data traffic from HA to CN (src: HA, dst: CN) {for BT}

CN configure the firewall(s) using EXT to let following traverse:

- for data traffic from HA to CN (src: HA, dst: CN) {for BT}
- for data traffic from HA to CN (src: HA, dst: CN) {for BT}

5. Home Agent behind a firewall

5.1. Route Optimization

In Figure 7, 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.

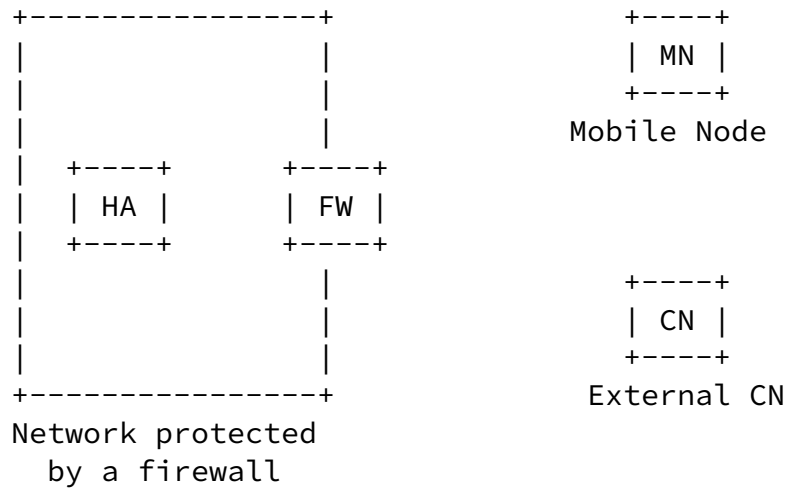


Figure 7: HA behind the firewall

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.

> For the BU (IPsec ESP in transport mode) traffic from MN to the HA, the MN installs rules using CREATE for the flow-id will be: SA: CoA, DA: HA, SPIx

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.

For the HoTI message (IPsec ESP in tunnel mode) from MN to the HA, the MN installs rules using CREATE the flow-id: SA: CoA, DA: HA, SPIx.

For the HoTI message from HA to the CN, the HA installs rules using CREATE for the flow-id: SA: HoA, DA: CN.

Detailed message flow between MN and HA is shown in Figure 8.

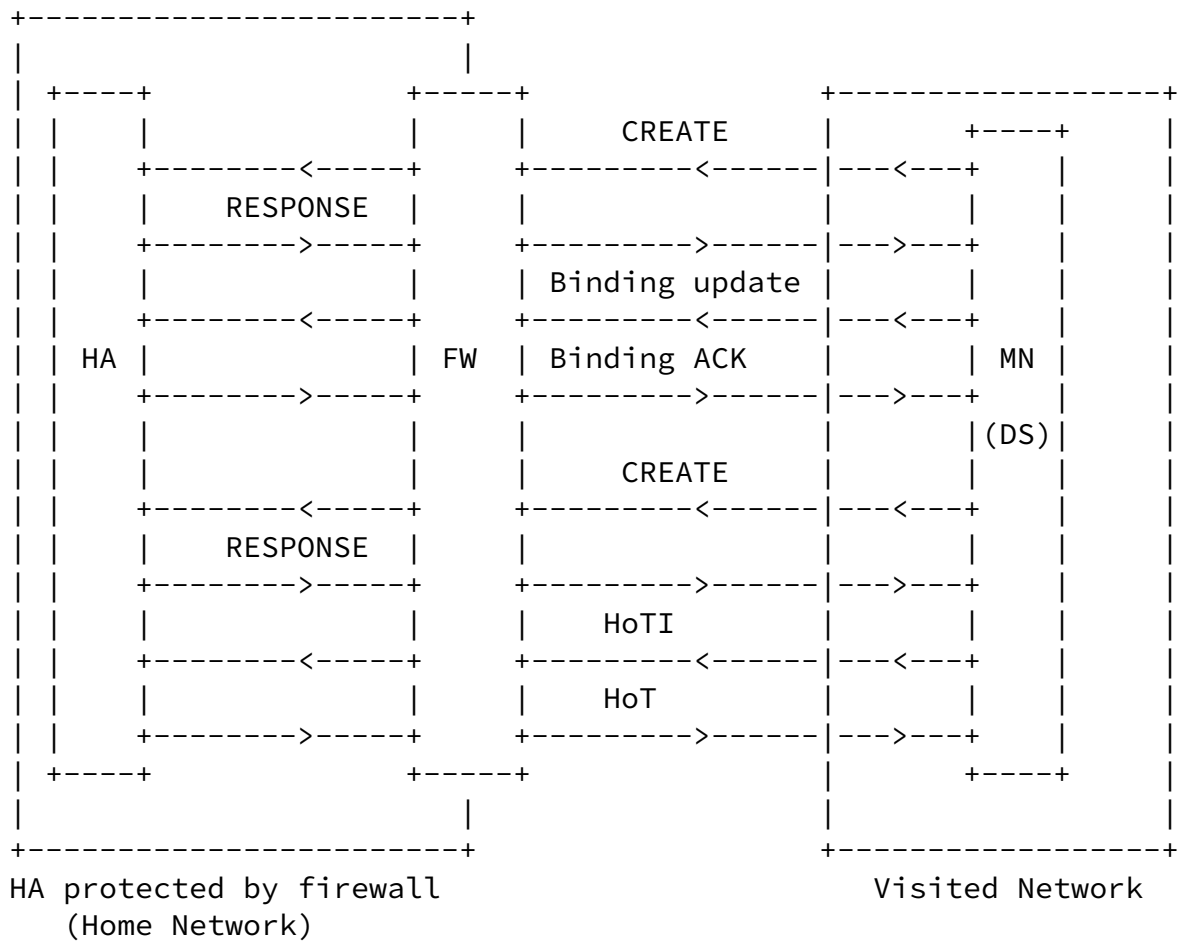


Figure 8: NSIS signaling for HA behind the firewall

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

5.2. Bi-directional tunneling

Here, it is necessary that the HA open pinholes for the data traffic from the CN using EXT. The CN is then allowed to send the data traffic through the FW. After intercepting a packet, the HA tunnels it to the MN. Figure 9 shows the message flow.

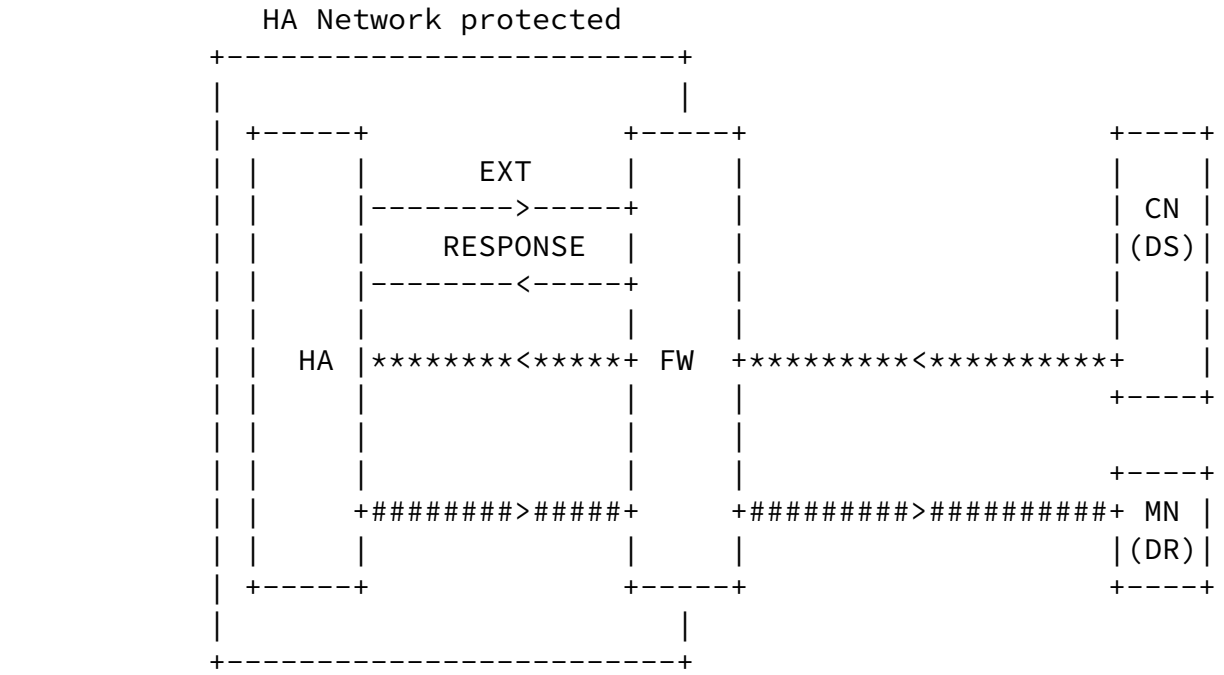


Figure 9: NSIS signaling for HA behind the firewall

For the data traffic from CN to HA, the HA installs rules using EXT for the flow-id: SA: CN, DA: HoA, SP: Data application port, DP: Data application port.

5.3. Operations when HA is behind a firewall

In summary, if a firewall is located at the edge of the MN's MSP, the MN configures the firewall(s) using CREATE to let following messages traverse:

- BU messages (src: CoA, dst: HA, SPIx) (IPsec ESP in transport mode) {for BU}

- HoTI messages (src: CoA, dst: HA, SPIx) (IPsec ESP in tunnel mode) {for RO}

The HA configures the firewall(s) using CREATE to let following messages traverse:

- HoTI messages (src: HoA, dst: CN) {for RO}

HA configure the firewall(s) using EXT to let following traverse:

- for data traffic from CN to HA (src: CN, dst: HA, SP: data application port, DP: data application port) {BT}

6. Additional Discussions

To support the operations described in this draft, it would be desirable if the NSIS NAT/FW NSLP has the ability to discover the presence and the characteristics (e.g., uplink or downlink filter) of firewalls. This will be useful in several cases.

For instance, it would be desirable if one could detect whether a firewall exists, if no, then NAT/FW NSLP will be unnecessary. Moreover, it is necessary to determine where (i.e., in which MIPv6 segment/scenario) is the firewall. This will be very useful to provide multiple firewall rules within a single signaling message exchange for multiple traffic modes (e.g., rules to allow BU and HoTI traverse). Current NAT/FW NSLP [2] specification does not provide this ability, however, we believe it would be useful to extend it to be able to discover the presence and characteristics of firewalls. This desired feature is already discussed in [8]:

> "A client MUST be able to create pinholes and specify the characteristics of the pinholes to be installed in the firewalls."

To enable the operations defined in this draft, some kind of interface between Mobile IPv6 and the NAT/FW NSLP is required. This interface notifies the NSLP about the MIP6 actions, for example the roaming into a new network and provides the required information (CoA, HoA, ...). This notification triggers the required operation.

The protocol uses a firewall detection approach to determine the current scenario and performs the pinhole creation process necessary for this case. After creation of the pinholes, MIP6 signaling is enabled to traverse possible firewalls.

The operation overview will be explained in more detail in future versions of this draft.

7. Security Considerations

The NAT/FW NSLP is in itself a very security sensitive service. A detailed description of possible threats and countermeasures are described in [2].

More details to authorization and authentication will be provided in the next version of this draft.

8. Acknowledgements

Parts of this document are a by-product of the ENABLE Project, partially funded by the European Commission under its Sixth Framework Programme. 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.

The authors would like to thank Hannes Tschofenig, Srinath Thiruvengadam, Martin Stiemerling, Cedric Aoun and Elwyn Davies for the discussions about the NAT/Firewall NSLP. Additionally, we would like to thank Marcus Brunner and Miquel Martin for their feedback.

9. References

9.1. Normative References

[1] Le, F., Faccin, S., Patil, B., and H. Tschofenig, "Mobile IPv6

and Firewalls: Problem Statement", RFC 4487, May 2006.

[2] Stiemerling, M., "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", draft-ietf-nsis-nslp-natfw-15 (work in progress), July 2007.

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

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

9.2. Informative References

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

[6] Brunner, M., "Requirements for Signaling Protocols", RFC 3726, April 2004.

[7] Lee, S., "Applicability Statement of NSIS Protocols in Mobile Environments", draft-ietf-nsis-applicability-mobility-signaling-07 (work in progress), July 2007.

[8] Bajko, G., "Requirements for Firewall Configuration Protocol", draft-bajko-nsis-fw-reqs-08 (work in progress), October 2007.

[9] Leung, K., "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-auth-protocol-07 (work in progress), September 2005.

Authors' Addresses

Niklas Steinleitner (editor)
University of Goettingen
Institute for Informatics
Lotzestr. 16-18
Goettingen 37083
Germany

Email: steinleitner@cs.uni-goettingen.de

Xiaoming Fu
University of Goettingen
Institute for Informatics
Lotzestr. 16-18
Goettingen 37083
Germany

Email: fu@cs.uni-goettingen.de

Franck Le
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213
USA

Email: franckle@cmu.edu

Full Copyright Statement

Intellectual Property

Acknowledgment

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