Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 20, 2009

S. Krishnan
Ericsson
N. Steinleitner
University of Goettingen
Y. Qiu
Institute for Infocomm Research
G. Bajko
Nokia

May 19, 2009

# Guidelines for firewall administrators regarding MIPv6 traffic
# draft-ietf-mext-firewall-admin-01

## Status of this Memo



## Abstract

This document presents some recommendations for firewall administrators to help them configure their existing firewalls in a way that allows in certain deployment scenarios the Mobile IPv6 signaling and data messages to pass through. For other scenarios, the support of additional mechanisms to create pinholes required for MIPv6 will be necessary. This document assumes that the firewalls in question include some kind of stateful packet filtering capability.

Table of Contents

## 1. Requirements notation

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 [RFC2119].

## 2. Introduction

Network elements such as firewalls are an integral aspect of a majority of IP networks today, given the state of security in the Internet, threats, and vulnerabilities to data networks. MIPv6 [RFC3775] defines mobility support for IPv6 nodes. Firewalls will interfere with the smooth operation of the MIPv6 protocol unless specific steps are taken to allow Mobile IPv6 signaling and data messages to pass through the firewall. The problems caused by firewalls to Mobile IPv6 are documented in [RFC4487].

This document presents some recommendations for firewall administrators to help them configure their firewalls in a way that allows the Mobile IPv6 signaling and data messages to pass through. This document assumes that the firewalls in question include some kind of stateful packet filtering capability. The static rules that need to be configured are described in this document. In some scenarios, the support of additional mechanisms to create pinholes required for MIPv6 signalling and data traffic to pass through will be necessary. A possible solution, describing the dynamic capabilities needed for the firewalls to create pinholes based on MIPv6 signalling traffic is described in a companion document [I-D.ietf-mext-firewall-vendor]. Other solutions may also be possible.

Some Mobile IPv6 signalling messages require the use of encryption to protect the confidentiality of the payload (e.g. the HoTI and HoT messages between the MN and the HA). The other signalling messages allow the use of encryption. If encryption is being used, it is not possible to inspect the contents of the signalling packets. For these messages to get through, a generic rule needs to be added in the firewall to let ESP packets through without further inspection.

## 3. Abbreviations

This document uses the following abbreviations:

- CN: Correspondent Node

- CoA: Care of Address
- CoTI: Care of Test Init
- HA: Home Agent
- HoA: Home Address
- HoTI: Home Test Init
- HoT: Home Test
- MN: Mobile Node
- RO: Route Optimization
- RRT: Return Routability Test

## 4. Home Agent behind a firewall

This section presents the recommendations for configuring a firewall that protects a home agent.

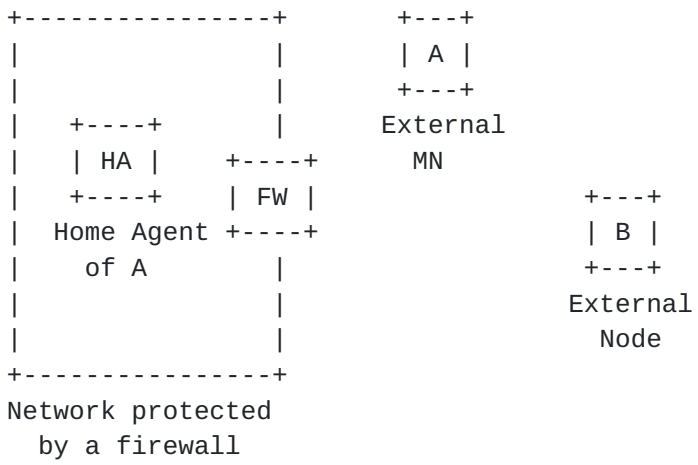


Figure 1: HA behind a firewall

For each type of traffic that needs to pass through this firewall, recommendations are presented on how to identify that traffic. The following types of traffic are considered

- Signaling between the MN and the HA
- IKEv2 signaling between MN and HA for establishing SAs

### 4.1. Signaling between the MN and the HA

The signaling between the MN and HA is protected using IPSec ESP. These messages are critical to the MIPv6 protocol and if these messages are discarded, Mobile IPv6 as specified today will cease to work. In order to permit these messages through, the firewall has to detect the messages using the following patterns.

```
Destination Address: Address of HA
Next Header: 50 (ESP)
Mobility Header Type: 5 (BU)
```

This pattern will allow the BU messages from MNs to HA to pass through.

### 4.2. IKEv2 signaling between MN and HA for establishing SAs

The MN and HA exchange IKEv2 signaling in order to establish the security associations. The security associations so established will later be used for securing the mobility signaling messages. Hence these messages need to be permitted to pass through the firewalls. The following pattern will detect these messages.

```
Destination Address: Address of HA
Transport Protocol: UDP
Destination UDP Port: 500
```

## 5. Correspondent Node behind a firewall

This section presents the recommendations for configuring a firewall if a node behind it should be able to act as Mobile IPv6 CN.

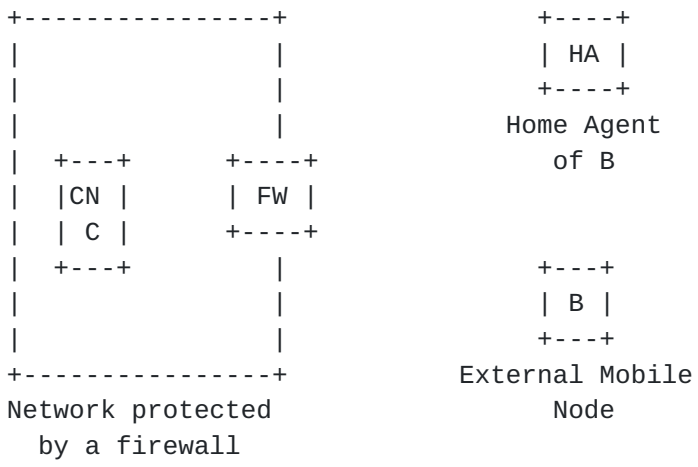

Figure 2: CN behind a firewall

For each type of traffic that needs to pass through this firewall, recommendations are presented on how to identify that traffic. The following types of traffic are considered

- Route optimization signaling between MN and CN through HA
- Route optimization signaling between MN and CN
- Binding Update from MN to CN
- Route Optimization data traffic from MN

## 5.1. Route optimization signaling between MN and CN through HA

Parts of the initial route optimization signaling has to pass through the HA, namely the HoTI and the HoT messages. Without assistance, the HoTI message from the HA to the CN is not able to traverse the firewall. When only a few priviledged nodes (like servers) are allowed to be contacted by outside nodes, then the following pattern will allow the HoTI messages to reach these nodes:

Destination Address: CN Address

Mobility Header Type: 1 (HoTI)

where CN Address describes the address(es) of the priviledged node(s). This pinhole allows the HoTI message from the HA to the CN to traverse the firewall. The HoT message from the CN to the MN through the HA can traverse the firewall without any assistance. Hence no pinhole is required.

## 5.2. Route optimization signaling between MN and CN

Route Optimization allows direct communication of data packets between the MN and a CN without tunnelling it back through the HA. To get route optimization work, the MN has to send a CoTI message directly to the CN, which response with a CoT message. However, a stateful firewall would prevent the CoTI message to pass through as there is no established state on the firewall. When only a few priviledged nodes (like servers) are allowed to be contacted by outside nodes, then the following pattern will allow the CoTI messages to reach these nodes:

Destination Address: CN Address

Mobility Header Type: 2 (CoTI)

where CN Address describes the address(es) of the priviledged node(s).The CoT message from the CN to the MN can traverse the firewall without any assistance. Hence no pinhole is required.

### 5.3. Binding Update from MN to CN

After successfully performing the return routability procedure, the MN sends the BU to the CN and expects the BA. Since this BU does not match any previous installed pinhole rules, an additional pinhole with the following format is required.When only a few priviledged nodes (like servers) are allowed to be contacted by outside nodes, then the following pattern will allow the BU messages to reach these nodes:

Destination Address: CN Address

Mobility Header Type: 5

where CN Address describes the address(es) of the priviledged node(s).This allows the BU to traverse the firewall and the BA can pass the firewall without any assistance. Therefore, the Binding Update sequence can be performed successfully.

### 5.4. Route Optimization data traffic from MN

Also the Route Optimization data traffic from MN directly to the CN can not traverse the firewall without assistance. A dynamically created pinhole such as the one specified in [I-D.ietf-mext-firewall-vendor] will allow this traffic to pass.

## 6. Mobile Node behind a firewall

This section presents the recommendations for configuring a firewall that protects the network a mobile node visiting.

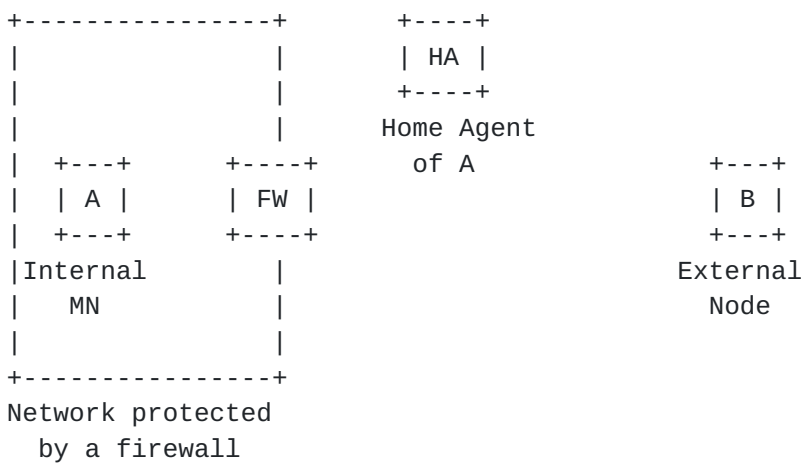


Figure 3: MN behind a firewall

For each type of traffic that needs to pass through this firewall, recommendations are presented on how to identify that traffic. The following types of traffic are considered

- Signaling between MN and HA
- Route Optimization Signaling between MN and CN
- IKEv2 signaling between MN and HA for establishing SAs

## 6.1. Signaling between MN and HA

As described in Section 4.1, the signaling between the MN and HA is protected using IPSec ESP. Currently, a lot of firewalls are configured to block the incoming ESP packets. Moreover, from the view of the firewall, both source and destination addresses of these messages from/to mobile node are variable. Fortunately, for a stateful firewall, if the initial traffic is allowed through the firewall, then the return traffic is also allowed. A mobile node is always the initiator for the BU. Since MN's CoA is not able to be known in advance, the firewall can use following patterns to permit these messages through.

Source Address: Visited subnet prefix

Destination Address: Address of HA
Next Header: 50 (ESP)
Mobility Header Type: 5 (BU)

This pattern will allow the Binding Update packets to pass through the firewall. Then the return packets (BA from HA to MN) will also able to pass through accordingly.

### 6.2. Signaling between MN and CN

Route Optimization allows direct communication of data packets between the MN and a CN without tunneling it back through the HA. It includes 3 pairs of messages: HoTI/HoT, CoTI/CoT and BU/BA. The first pair can pass through the firewall using the pattern described in section 5.1. Here we discuss CoTI/CoT and BU/BA messages. Following pattern permits these messages through the firewall.

Source Address: Visited subnet prefix
  Mobility Header Type: 2 (CoTI)

Source Address: Visited subnet prefix
  Mobility Header Type: 5 (BU)

This pattern allows the initial messages (CoTI and BU) from the MN to the CN pass through the firewall. The return messages (CoT and BA) from the CN to the MN can also passes through the firewall accordingly.

### 6.3. IKEv2 signaling between MN and HA for establishing SAs

The MN and HA exchange IKEv2 signaling in order to establish the security associations. The security associations so established will later be used for securing the mobility signaling messages. Due to variable source/destination IP addresses and MN always as initiator, the following pattern will let the negotiation pass.

Source Address: Visited subnet prefix
Transport Protocol: UDP
Destination UDP Port: 500

## 7. Related documents

There are other IETF published documents that provide recommendations for firewall configuration that can affect Mobile IPv6 messages. [RFC4890] that provides recommendations for filtering ICMPv6 messages (especially Section 4.3.2). [RFC4942] describes security issues present in IPv6 and related protocols (especially Sections 2.1.2 and 2.1.15).

## 8. Acknowledgements

The authors would like to thank the following members of the MIPv6 firewall design team for contributing to this document: Hannes

Tschofenig, Hesham Soliman, Yaron Sheffer, and Vijay Devarapalli. The authors would also like to thank William Ivancic, Ryuji Wakikawa, Jari Arkko, Henrik Levkowetz, Pasi Eronen and Noriaki Takamiya for their thorough reviews of the document and for providing comments to improve the quality of the document.

## 9. IANA Considerations

This document does not require any IANA action.

## 10. Security Considerations

This document specifies recommendations for firewall administrators to allow Mobile IPv6 traffic to pass through unhindered. Since some of this traffic is encrypted it is not possible for firewalls to discern whether it is safe or not. This document recommends a liberal setting so that all legitimate traffic can pass. This means that some malicious traffic may be permitted by these rules. These rules may allow the initiation of Denial of Service attacks against Mobile IPv6 capable nodes (the MNs, CNs and the HAs).

## 11. References

### 11.1. Normative References

[I-D.ietf-mext-firewall-vendor] Krishnan, S., Sheffer, Y., Steinleitner, N., and G. Bajko, "Guidelines for firewall vendors regarding MIPv6 traffic", draft-ietf-mext-firewall-vendor-00 (work in progress), October 2008.

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

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4487] Le, F., Faccin, S., Patil, B., and H. Tschofenig, "Mobile IPv6 and Firewalls: Problem Statement", RFC 4487, May 2006.

### 11.2. Informative References

[RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, May 2007.

[RFC4942]  Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/
Co-existence Security Considerations", RFC 4942,
September 2007.

## Authors' Addresses

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

Niklas Steinleitner
University of Goettingen
Lotzestr. 16-18
Goettingen
Germany

Email: steinleitner@cs.uni-goettingen.de

Ying Qiu
Institute for Infocomm Research
21 Heng Mui Keng Terrace
Singapore

Phone: +65-6874-6742
Email: qiuying@i2r.a-star.edu.sg

Gabor Bajko
Nokia

Email: gabor.bajko@nokia.com

## Full Copyright Statement



## Intellectual Property