

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 7, 2008

S. Krishnan
Ericsson
N. Steinleitner
University of Goettingen
Y. Qiu
Institute for Infocomm Research
July 6, 2007

Firewall Recommendations for MIPv6
draft-krishnan-mip6-firewall-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 7, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft

MIPv6 Firewall BCP

July 2007

Abstract

This document presents some recommendations for firewall administrators to help them configure their firewalls in a way that allows 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.

Table of Contents

1.	Requirements notation	3
2.	Introduction	4
3.	Home Agent behind a firewall	5
3.1.	Signaling between the MN and the HA	5
3.2.	Route optimization signaling between MN and CN through HA	5
3.3.	IKEv2 signaling between MN and HA for establishing SAs . .	6
3.4.	Data traffic from and to MN passing through the HA	6
4.	Correspondent Node behind a firewall	7
4.1.	Route optimization signaling between MN and CN through HA	7
4.2.	Route optimization signaling between MN and CN	7
4.3.	Binding Update from MN to CN	8
4.4.	Route Optimization data traffic from MN	8
4.5.	Bi-directional tunnelled data traffic from the MN to the CN through HA	8
5.	Mobile Node behind a firewall	10
5.1.	Signaling between MN and HA	10
5.2.	Signaling between MN and CN	10
5.3.	IKEv2 signaling between MN and HA for establishing SAs . .	11
5.4.	Data traffic from and to the MN	11
6.	Contributors	12
7.	IANA Considerations	13
8.	Security Considerations	14
9.	Normative References	15
	Authors' Addresses	16
	Intellectual Property and Copyright Statements	17

Internet-Draft

MIPv6 Firewall BCP

July 2007

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. Since firewalls are not aware of MIPv6 protocol details, they will probably interfere with the smooth operation of the protocol. 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 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.

[3.](#) Home Agent behind a firewall

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

- o Signaling between the MN and the HA
- o Route optimization signaling between MN and CN through HA
- o IKEv2 signaling between MN and HA for establishing SAs
- o Data traffic from and to MN passing through the HA

[3.1.](#) Signaling between the MN and the HA

The signaling between the MN and HA is protected using IPSec ESP. These messages are encrypted and hence are not inspectable by firewalls. So the firewall has to either permit all these messages or discard all of them. But 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 pattern.

Destination Address: Address of HA
IP payload protocol number: 50 (ESP)

This pattern will allow the BU messages from MNs to HA and BA messages from the HA to the MNs to pass through. It will also allow the HoTI and HoT messages (related to route optimization) between the MN and the HA to pass through.

[3.2.](#) Route optimization signaling between MN and CN through HA

Route Optimization allows direct communication of data packets between the MN and a CN without tunneling it back through the HA. In order for route optimization to work, part of the initial signaling has to pass through the HA. The following pattern will allow these messages to pass through.

Destination Address: HoA of MN
Mobility Header Type: 3

This pattern allows the HoT message from the CN to the MN's HoA to pass through the firewall. The HoTI message from the MN to the CN through the HA usually passes through the firewall without any

problems. Hence no specific pattern is recommended. If the firewall does not have the capability to recognize the mobility header type, it needs to at least filter on the IP payload protocol type 135 (Mobility Header) in order to limit the scope of this filter rule.

[3.3.](#) 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. 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

[3.4.](#) Data traffic from and to MN passing through the HA

If a CN tries to initiate traffic to an MN, a stateful firewall would prevent these connection requests to pass through as there is no established state on the firewall. Since MNs do not usually provide services, this is not usually a problem. But if this is necessary to do, the pattern to look for is

Destination Address: MN HoA

Allowing this traffic might allow any kind of traffic, including malicious traffic, to pass through unfiltered to the MN. This would expose the MN to any type of possibly malicious traffic, resulting in a denial of service or exploitation of known security vulnerabilities. This practice is NOT RECOMMENDED.

[4.](#) 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. 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

- o Route optimization signaling between MN and CN through HA
- o Route optimization signaling between MN and CN
- o Binding Update from MN to CN
- o Route Optimization data traffic from MN
- o Bi-directional tunnelled data traffic from the MN to the CN through HA

[4.1.](#) 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. The following pattern will allow these messages to traverse.

Destination Address: CN Address

Mobility Header Type: 1

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.

[4.2.](#) 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. The following pinhole will allow the CoTI message to traverse.

Destination Address: CN Address

Mobility Header Type: 2

The CoT message from the CN to the MN can traverse the firewall without any assistance. Hence no pinhole is required.

[4.3.](#) 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.

Destination Address: CN Address

Mobility Header Type: 5

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.

[4.4.](#) 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. But as we have configured the firewall to allow the BU message from MN to the CN to traverse the firewall, the Route Optimization data traffic is able to pass through as it also matches the pinhole installed for the BU.

Therefore, no additional pinhole rules are required.

[4.5.](#) Bi-directional tunnelled data traffic from the MN to the CN through HA

If a MN tries to initiate traffic to a CN through the HA using bi-directional tunnelling, a stateful firewall would prevent these connection requests to pass through as there is no established state on the firewall. This is usually a problem as CNs often provide services. A solution is to static configure the firewall to let this traffic pass through. However, this is only an acceptable option if it is not necessary to open an all-embracing pinhole, e.g. if the destination ports are well-known. In this case, the pinhole has to look like

Destination Address: CN Address

Destination Port: Application Ports

If the ports are unknown, it is necessary to install a pinhole with only the Destination Address as pattern. Allowing this traffic might allow any kind of traffic, including malicious traffic, to traverse to the CN. Allowing this traffic might allow any kind of traffic, including malicious traffic, to pass through unfiltered to the CN. This would expose the CN to any type of possibly malicious traffic, resulting in a denial of service or exploitation of known security vulnerabilities. This practice is NOT RECOMMENDED

[5.](#) Mobile Node behind a firewall

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

- o Signaling between MN and HA
- o Route Optimization Signaling between MN and CN
- o IKEv2 signaling between MN and HA for establishing SAs
- o Data traffic from and to MN

[5.1.](#) Signaling between MN and HA

As described in [Section 3.1](#), 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 pattern to permit these messages through.

Source Address: Visited subnet prefix
IP payload protocol number: 50 (ESP)

This pattern will allow the initial packets (e.g. BU from MNs to HA, HoTI, etc.) to pass through the firewall. Then the return packets (BA from HA to MN, HoT) is also able to pass through accordingly.

[5.2.](#) 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
IP payload protocol number: 135 (Mobility Header)

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 pass through the firewall accordingly.

[5.3.](#) 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

[5.4.](#) Data traffic from and to the MN

After sending the home binding update, every traffic packet between MN and HA will be encapsulated by ESP. As described in [section 5.1](#), the firewall allows these packets pass through. However, if a CN tries to initiate traffic to an MN, a stateful firewall would prevent these connection requests to pass through as there is no established state on the firewall. We may use following steps to establish a channel state between MN and CN:

1. When detecting BU message from MN to CN with protocol number 135 and mobility header type 5, the firewall extracts the home address from the destination option.

2. Firewall adds a security rule to its table with following pattern.

Destination Address: CoA
Source Address: CN
Routing Header Type 2 Address: HoA

Thereafter any packets to MN will be filtered by above pattern.

Krishnan, et al. Expires January 7, 2008 [Page 11]

Internet-Draft MIPv6 Firewall BCP July 2007

6. Contributors

This document is one of the deliverables of the MIPv6 firewall design. The following members of the team were involved in the creation of this document.

Hannes Tschofenig Hannes.Tschofenig@gmx.net

Gabor Bajko Gabor.Bajko@nokia.com

Suresh Krishnan suresh.krishnan@ericsson.com

Hesham Soliman solimanhs@gmail.com

Yaron Sheffer yaronf@checkpoint.com

Qiu Ying qiuying@i2r.a-star.edu.sg

Ram Vishnu vishnu@motorola.com

Niklas Steinleitner steinleitner@cs.uni-goettingen.de

Vijay Devarapalli vijay.devarapalli@AzaireNet.com

[7.](#) IANA Considerations

This document does not require any IANA action.

8. 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). Especially the rules specified in [Section 3.4](#) and [Section 4.5](#) are broadly defined

and hence possess the most potential for abuse. Hence, if these rules are implemented, the firewalls SHOULD be configured to rate-limit such traffic on a per-destination basis. This would allow the firewall to mitigate possible denial of service attacks on the endpoints. Please note that such measures would not mitigate other potential security issues.

Krishnan, et al.	Expires January 7, 2008	[Page 14]
------------------	-------------------------	-----------

Internet-Draft	MIPv6 Firewall BCP	July 2007
----------------	--------------------	-----------

[9.](#) Normative References

- [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.

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

Internet-Draft

MIPv6 Firewall BCP

July 2007

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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