Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2012

S. Krishnan
Ericsson
Y. Sheffer
Check Point
N. Steinleitner
University of Goettingen
G. Bajko
Nokia

October 17, 2011

Guidelines for firewall vendors regarding MIPv6 traffic
draft-ietf-mext-firewall-vendor-05

Abstract

This document presents some recommendations for firewall vendors to help them implement their firewalls in a way that allows Mobile IPv6 and DSMIPv6 signaling and data messages to pass through. This document describes how to implement stateful packet filtering capability for MIPv6 and DSMIPv6.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 19, 2012.

Copyright Notice

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. 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 vendors to help them implement their firewalls in a way that allows Mobile IPv6 signaling and data messags to pass through. This document describes how to implement stateful packet filtering capability for MIPv6.

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. MIPv6 Firewall Primitives

3.1. Requirements

This document assumes that the firewalls are capable of deep packet inspection at least until the mobility header. This implies that they are capable of parsing ICMPv6 packets and options in addition to understanding the mobility header. It also assumes that the firewalls are capable of creating filters based on arbitrary fields based on the contents of a signaling packet.

3.2. Detecting and parsing the Mobility Header

The Mobility Header is the basic primitive in all MIPv6 signaling messages. Thus the firewalls need to be able to recognize the presence of the mobility header and be able to parse the contents of the Mobility Header. The MH is described in section 6.1 of [RFC3775]

and the format of the same is described in section 6.1.1 of [RFC3775]. Firewalls need to be able to at least understand the contents of the MH Type field that describes the type of signaling message carried.

3.3. Parsing Mobility Options

The Mobility Header can carry additional information in the form of mobility options as described in section 6.2 of [RFC3775] and section 3 of [RFC5555]. Some of these mobility options need to be understood for proper creation of state on the firewalls. Hence firewalls must be able to parse the mobility options defined in [RFC3775] and [RFC5555].

4. Allowing signaling response packets

The MIPv6 signalling messages are usually performed as a request-response pair. The request message is usually allowed by setting up a static firewall rule to allow the traffic to pass through. The response message on the other hand can be dynamically allowed if the firewall can automatically setup a filter for the response packets when the request packet passes through. This is not trivial, but fortunately is straightforward. There are 3 message pairs that are of importance to MIPv6 signaling. They are the BU/BA, HoTI/HoT and CoTI/CoT pairs. When the first message in the pair traverses the firewall in one direction, the firewall must setup a filter rule to allow the second message through in the other direction.

Consider a packet that matches a static rule configured on a firewall

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

This rule allows a binding update message from a MN to pass through to the HA. Once a packet that matches this rule passes through the firewall, the firewall must setup a dynamic filter for the return packet

```
Source Address: Destination Address from Packet

Destination Address: Source Address from Packet
Next Header: 50 (ESP)
Mobility Header Type: 6 (BA)
```

This rule ensures that the return BA packet will pass through unhindered. The rules can be generalized as summarized in the table

below.

Passing packet MH Type	Setup return filter with MH Type
Mobility Header Type:1(HoTI)	Mobility Header Type:3(HoT)
Mobility Header Type:2(CoTI)	Mobility Header Type:4(CoT)
Mobility Header Type:5(BU)	Mobility Header Type:6(BA)

Table 1: Message Pairs in MIPv6

Such dynamic rules can be timed out after a configurable period STATEFUL_PINHOLE_LIFETIME, unless renewed by new mobility messages. This document recommends that the default value of STATEFUL_PINHOLE_LIFETIME be set to 30 seconds.

These dynamic rules MUST be immediately deleted after the return message passes through. e.g. Once a return HoT message for a HoTI passes through, the pinhole must be immediately removed.

A DSMIPv6 client [RFC5555] having been configured with only a v4 CoA, will tunnel the MIP6 signaling messages to the HA's IPv4 address using its IPv4 CoA. These messages are either IP-in-IP encapsulated (protocol number 4) or UDP&IP encapsulated and sent to the destination UDP port number 4191.

The firewall SHOULD understand the Binding Update and Binding Acknowledgement Message Extensions and check the status of the F flag. If the F flag is set to zero in both the BU and the BA, the firewall MUST set up a dynamic filter for the return packets:

Destination Address: IPv4 CoA of the MN
Protocol: 4 (IP-in-IP)
Source Address: IPv4 address of the HA

When the F flag is set to 1 in either the BU and BA, the firewall does not need to take any special action, as the signaling packets will be UDP encapsulated.

5. Allowing data packets based on signaling

Once the MIPv6 signaling completes, the data traffic can begin to flow. The traffic filters for the data traffic can be inferred from the contents of the signaling messages that setup the session. This section describes how firewalls can intelligently setup filters for

data traffic based on signaling traffic.The following example describes how to setup a filter for allowing incoming route optimized messages from a CN to an MN after the MN sent a BU message to a CN.

When the BU message from MN to CN (MH Type 5) traverses through the firewall the firewall extracts the home address (HoA) from the Home Address Option (section 6.3 of [RFC3775]) of the packet.

The firewall adds the following rule in order to let the return traffic pass.

Destination Address: Source Address of the packet (MN CoA)
Source Address: Destination Address of packet (CN)
Routing Header Type 2 Address: HoA

This pattern allows all route optimized traffic coming from the CN to the MN to pass through.

Additionally, the firewall adds a second rule in order to let the data traffic from the MN to the CN pass through.

Source Address: Source Address of the packet (MN CoA)
Destination Address: Destination Address of packet (CN)
Next Header: IPv6 Destination Options Header(60)
Home Address Dest. Option: MN HoA

This pattern allows all route optimized traffic coming from the MN to the CN to pass through.

A firewall protecting the HA can add the following rule on reception of a HA binding update, in order to let the incoming bi-directional tunneled traffic pass.

Destination Address: Source Address of the packet (MN HoA)
Source Address: Destination Address of packet (CN)

6. 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, Qiu Ying, and Vijay Devarapalli. The authors would also like to thank William Ivancic, Ryuji Wakikawa, Jari Arkko, Henrik Levkowetz, Pasi Eronen, Noriaki Takamiya and Arnaud Ebalard for their thorough reviews of the document and for providing comments to improve the quality of the document.

7. IANA Considerations

This document does not require any IANA action.

8. Security Considerations

This document specifies recommendations for firewall vendors to allow Mobile IPv6 traffic to pass through unhindered. This document recommends a liberal setting of firewall rules so that all legitimate traffic may be allowed to 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).

One of the main goals of any firewall is to prevent unsolicited traffic from entering the network. The proposed solution allows such traffic into the network, albeit with a number of restrictions.

In a typical enterprise environment, an administrator cannot distinguish Mobile IPv6 capable nodes from other nodes. In such a situation any node in the protected network may end up receiving unsolicited packets from outside the firewall. The risk in this case is that such packets could trigger unknown vulnerabilities in any of these nodes, causing denial-of-service or worse attacks. This issue is compounded in a mobile service provider environment by the risks specific to such environments like endpoint battery exhaustion and spectrum misuse.

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.

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

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

Yaron Sheffer
Check Point
5 Hasolelim St.
Tel Aviv 67897
Israel

Email: yaronf@checkpoint.com

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

Email: steinleitner@cs.uni-goettingen.de

Gabor Bajko
Nokia

Email: gabor.bajko@nokia.com