MEXT Working Group
Internet Draft
Intended status: Standards Track
Expires: August 2010

X.Cui
Huawei

February 10, 2010

# Stateful Firewall Traversing for Route Optimization
## draft-cui-mext-firewall-traversing-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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/1id-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 August 10, 2010.

Abstract

This document presents a new approach for the scenario where the correspondent node is in a network protected by stateful firewall. The approach extends the mobility management procedure and enables the Return Routability related messages to traverse the stateful firewall and Route Optimization may also be achieved well in such scenario.

Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

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].

Table of Contents

## 1. Introduction

Mobile IP [RFC3775] is standardized to support mobility of IPv6 and the Mobile Node with support of Mobile IP can keep the established session when it is moving.

Firewall is security device that can protect IP nodes inside the security domain and resist hostile attacks.

Mobility and security are the most important features of IPv6 but in current specifications they can not cooperate well.

As specified in [RFC4487], many issues will happen in some scenarios. Section 5.2 of [RFC4487] shows the scenario where the correspondent node is in a network protected by firewall. Some analyses for this scenario are also provided in [RFC4487].

In principle, the issues may be resolved in two different ways, extension of firewall or extension of mobility management.

One approach, which is based on extensions and configuration of static firewall, is introduced in [draft-ietf-mext-firewall-admin] and [draft-ietf-mext-firewall-vendor]. But at present many network administrators use stateful firewall as the security device and the configuration of static firewall is not welcomed in many scenarios.

This document presents another approach, which is based on the combination of extension of Mobility management and stateful firewall. In this approach the requirements of firewall may be simplified and the complex configuration on firewall may be avoided.

## 2. Terminology

All the mobility related terms used in this document are to be interpreted as defined in the Mobile IPv6 specification [RFC3775] and Problem Statement of Mobile IPv6 and Firewalls [RFC4487].

## 3. Scenario and Solution Consideration

### 3.1. Scenario

This document focuses on the scenario described in section 5.2 of [RFC4487]. In this scenario the Corresponding Node is protected by the firewall.

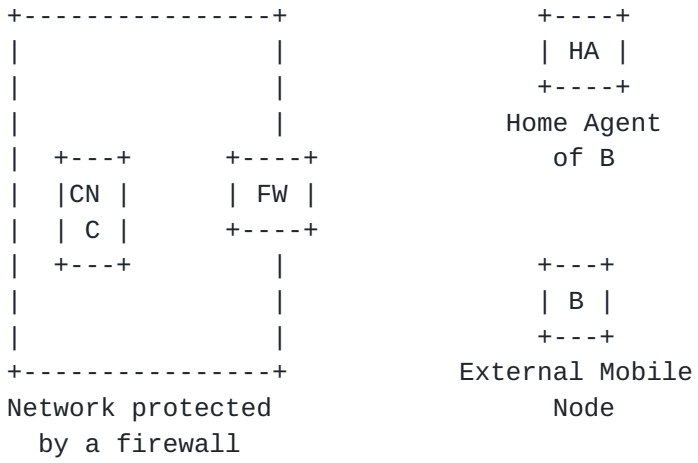



Figure 1 CN Is in a Network Protected by Firewall.

Since the stateful firewall is the most common firewall device in current network, this draft takes the fact as a precondition.

The stateful firewalls implement the Stateful packet filtering function which is defined in [RFC2647] as "forwarding or rejecting traffic based on the contents of a state table maintained by a firewall." [RFC2647] also specifies that "devices using stateful packet filtering will only forward packets if they correspond with state information maintained by the device about each connection". Additionally, the connection is established by data exchanged between hosts.

In such scenario, the connection between corresponding node C and external node B is established in the firewall based on the address of corresponding node C and home address of mobile node B. At this stage the corresponding node C may send packets to home address (by existing connection state) and care of address (by dynamically established connection state) of external mobile node B. The external node B can send packets to corresponding node only with its home address but can not send packets to C with its care of address,

because there is no corresponding connection state for the care of address of node B.

### 3.2. Solution Consideration

This document presents a new approach for the above scenario. The solution extends the route optimization establishment procedure and use 'Hole Punching' techniques to set up a connection state for care of address of external node B.

The message flow of this solution is as follows:

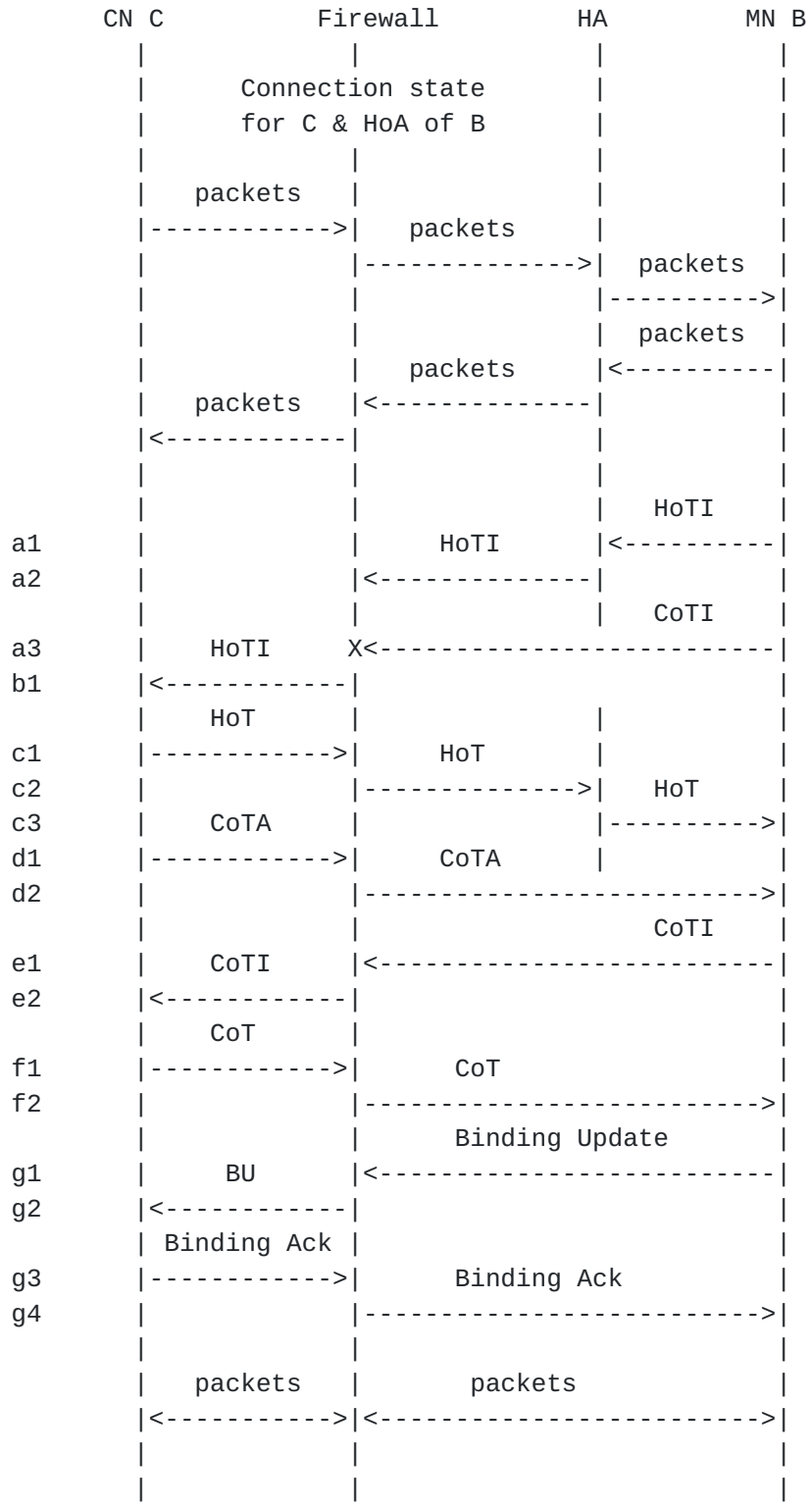



Figure 2 Route Optimization Extension for Firewall.

The detailed descriptions are as follows:

At the initiatory stage, the stateful firewall establishes a connection state for the internal node (i.e., CN C) and external node (i.e., MN B). CN C can send packets to MN B by home address of MN B, which is included in the destination IP address field of the packet. Since the firewall maintains the connection state, the packets are allowed to go through the firewall. MN B can also send packets to CN C by home address of MN B, which is included in the source IP address field of the packet. Since the firewall maintains the connection state, the packets are also allowed to go through the firewall.

(a1~a3) MN B initiates the Return Routability procedure and sends HoTI and CoTI messages to CN C as specified in [RFC3775], with the exception that the Punching Flag and Alternate Care-of Address Option are included in the HoTI message. HoA of MN B is included in the source IP address field of HoTI and CoA of MN B is included in the source IP address field of CoTI message.

(b1) Since the firewall maintains the state of HoA connection (i.e., between the address pair of CN and HoA of MN), the HoTI message is allowed to go through the firewall. But the firewall doesn't maintain the state of CoA connection (i.e., between the address pair of CN and CoA of MN), the CoTI message is not allowed to go through the firewall. The firewall drops the CoTI packet.

(c1~c3) CN C receives the HoTI message and replies a HoT message as specified in [RFC3775]. The HoT message can traverse the firewall and arrive at MN B.

(d1~d2) The Punching Flag included in HoTI message trigger the CN B to respond a Care-of Test Allowance (CoTA) message to the address which is included in the Alternate Care-of Address Option. CN C copies the care of address from the HoTI message and sends the Care-of Test Allowance message to the care of address of MN B. Since the stateful firewall permits the protected node to send packets to the outside network, the CoTA message can traverse the firewall and arrive at MN B. The firewall simultaneously establishes a new connection state for the care of address of MN B in its connection state table.

(e1~e2) MN B receives the CoTA message and immediately resends the CoTI message to CN C. Since there is corresponding connection state in the firewall at this time, the CoTI can go through the firewall.

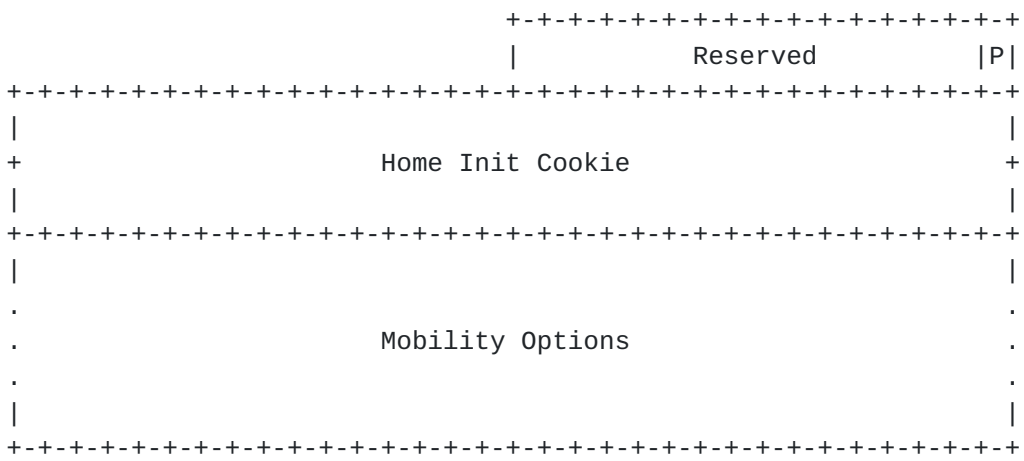
(f1~f2) The CN C receives the CoTI message and responds CoT as specified in [RFC3775]. The CoT packet goes through the firewall and arrives at MN B.

(g1~g4) Normal corresponding binding update is implemented as specified in [RFC3775].

After the Route Optimization is established, packets can be delivered without the involvement of Home Agent.

## 4. Messages Formats

### 4.1. Extension of HoTI Message

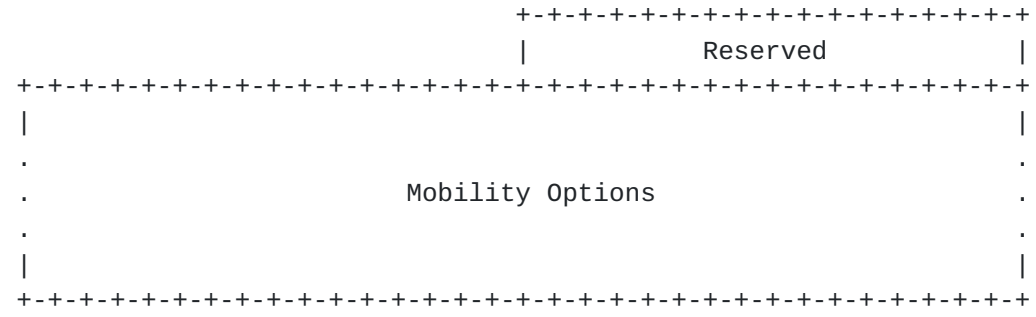



A new flag (P)unching is added in Home Test Init message to request firewall punching and Alternate Care-of Address option SHOULD be included in extended HoTI message.

When the P flag is set to a value of 1 the receiver of HoTI message SHOULD respond CoTA message to the care of address included in the same HoTI message.

### 4.2. Care-of Test Allowance Message

A node in the protected network uses the Care-of Test Allowance (CoTA) message to punch a hole in the stateful firewall for the Return Routability procedure. The Care-of Test Allowance message uses the MH Type value TBD1. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:




Reserved

16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand.

## 5. Security Considerations

The security must be carefully considered for this solution. Since the attacker can forge the Home Test Init message and cheat the firewall for a dangerous hole, the protected node must carefully check the HoTI message and some security extensions may be integrated in this solution.

## 6. IANA Considerations

TBD1 is a new Mobility Header type value introduced in this document. IANA is requested to assign the new type value for the Care-of Test Allowance message.

## 7. Acknowledgments

TBD.

## 8. References

### 8.1. 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.

### 8.2. Informative References

[RFC2647] Newman, D., "Benchmarking Terminology for Firewall Performance", RFC 2647, August 1999.

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

Author's Addresses

Xiangsong Cui
Huawei Technologies
KuiKe Bld., No.9 Xinxi Rd.,
Shang-Di Information Industry Base,
Hai-Dian District, Beijing, P.R. China, 100085

Email: Xiangsong.Cui@huawei.com