INTERNET DRAFT
File: draft-ietf-mip6-firewalls-00.txt
Expires: February 2005

Franck Le
Stefano Faccin
Basavaraj Patil
Nokia
H. Tschofenig
Siemens
August 2004

Mobile IPv6 and Firewalls
Problem statement

Status of this Memo

Abstract

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. IP networks today are predominantly based on IPv4 technology and hence firewalls have been designed for these networks. Deployment of IPv6 networks is currently progressing, albeit at a slower pace. Firewalls for IPv6 networks are still maturing and in development.

Mobility support for IPv6 has now been standardized as specified in RFC3775 [MIP6]. Given the fact that Mobile IPv6 is a recent

standard, most firewalls available for IPv6 networks today do not support Mobile IPv6.

Unless firewalls are aware of Mobile IPv6 protocol details, these security devices will interfere in the smooth operation of the protocol and can be a detriment to deployment. This document presents in detail some of the issues that people deploying IPv6 networks which include firewalls should consider when expanding the scope to support Mobile IPv6 as well.

The issues are not only applicable to firewalls protecting enterprise networks, but are also applicable in 3G mobile networks such as GPRS/UMTS and cdma2000 networks where packet filters are implemented in the GGSN in GPRS/UMTS networks and the PDSN in cdma2000 networks.

The goal of this Internet draft is to highlight the issues with firewalls and Mobile IPv6 and act as an enabler for further discussion. Issues identified here can be solved by developing appropriate solutions in the MIP6 WG.

1. Introduction

Mobile IPv6 enables IP mobility for IPv6 nodes. It allows a mobile IPv6 node to be reachable via its home IPv6 address irrespective of any link that the mobile attaches to. This is possible as a result of the extensions to IPv6 defined in the Mobile IPv6 specification [MIP6].

Mobile IPv6 protocol design also incorporates a feature termed as Route Optimization. This set of extensions is a fundamental part of the protocol that enables optimized routing of packets between a Mobile Node and its correspondent node and therefore the performance of the communication.

In most cases, current firewall technologies however do not support Mobile IPv6 or are even unaware of Mobile IPv6 headers and extensions. Since most networks in the current business environment deploy firewalls, this may prevent future large-scale deployment of the Mobile IPv6 protocol.

This document presents in detail some of the issues that firewalls present for Mobile IPv6 deployment, as well as the impact of each issue.

2. Background information

2.1 Overview of stateful inspection packet filters

One set of issues is related to the way IP addresses are used in Mobile IP, and the way state information is created and maintained in stateful inspection packet filters. We refer to the internal node as the node connected to the network protected by the firewall, and to external node as the node outside the boundaries of the network protected by the firewall.

Subsequently, we describe how stateful inspection packet filters work:

When a MN connects to a TCP socket on another host in the Internet, it provides, at the connection setup, the socket (IP address and port) on which it expects to receive a response.

When that SYN packet is routed through the firewall, the firewall makes an entry in its state table containing the destination socket and the response socket, and then forwards the packet to the destination.

When the response comes back, the filter looks up the packets

source and destination sockets in its state table: If they match an expected response, the firewall lets the packet pass. If no table entry exists, the packet is dropped since it was not requested from inside the network.

The filter removes the state table entries when the TCP close session negotiation packets are routed through, or after some period of delay, usually a few minutes. This ensures that dropped connections do not leave table holes open.

For UDP, similar state is created but since UDP is connectionless and the protocol does not have indication of the beginning nor the end of a session, the state is based only on timers.

2.2 Mobile IP6 issues with packet filtering in 3G networks

In 3G networks, packet filtering functionalities may be implemented to prevent malicious nodes from flooding or launching other attacks against the 3G subscribers. The packet filtering functionality of 3G networks are further described in [3GPP].

In such case, packet filters are set up and applied to both uplink and downlink traffic: outgoing and incoming data not matching the packet filters is dropped.

The issues described in the following sections thus also apply to 3G networks.

3. Analysis of various scenarios involving MIP6 nodes and firewalls

The following section describes various scenarios involving MIP6 nodes and firewalls and presents the issues related to each scenario.

In the following section, the node in a network protected by a firewall will be refered to the inner node, and the node in the external network will be refered to the external node.

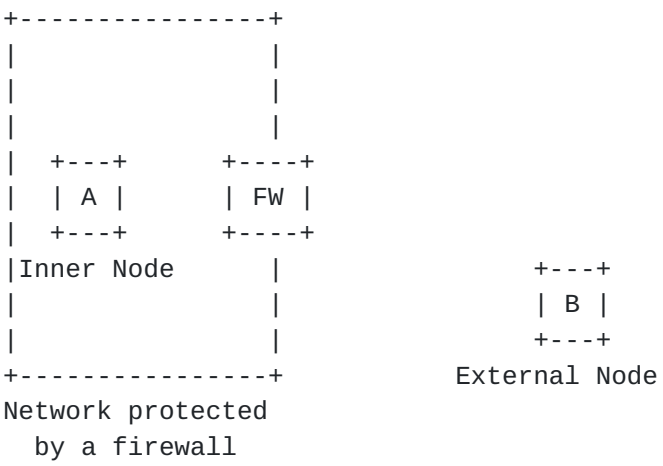

Figure 1. Illustration of inner and external nodes

3.1 Scenario when the external node is a Mobile Node

Let's assume a communication between an internal node A, and an external Mobile Node B. The node A is in a network protected by a firewall, and node B may also be protected by a firewall but this section focuses on the issues related to the firewall protecting the node A. Issues related to the firewall protecting node B are further described in the following section.

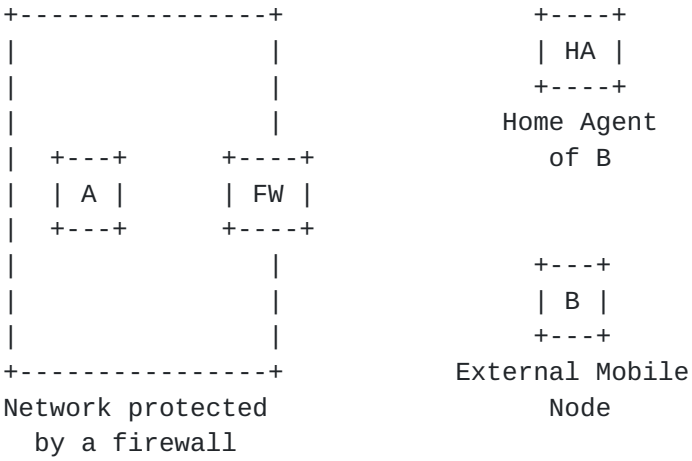

Figure 2. Issues between MIP6 and firewalls
when a firewall is protecting the CN

3.1.1 Return Routability Test sp

As specified in Mobile IPv6 [MIP6], a MN should base its communication on the Home IP address of B, IP HoA B, and not on the

care-of-address that B obtains while attached to a link other than its home link.

The state created by the stateful inspection packet filter protecting A is therefore initially based on the IP address of A (IP A) and the home address of the node B (IP HoA B).

If the Mobile Node B is connected to its home link, packets are directly exchanged between the nodes A and B. If the Mobile Node B is attached to any other link than its home link (in which case it has a care-of-address), the session can still be maintained by having the MN tunnel the traffic destined to the CN (Node A) via its home agent [MIP6]. Packets forwarded by the Home Agent to the node A will have the source IP address indicating the Home IP address of B and the destination IP address indicating the IP address of A. Such packets can thus pass the firewall functionality protecting A.

However nodes A and B might be topologically close to each other while B's Home Agent may be far away, resulting in a trombone effect that can create delay and degrade the performance.

Route Optimization is a feature that enables a MN to communicate directly with its CN, without involving the MN's Home Agent in the data path. So in the current scenario the MN B can initiate the route optimization procedure with Node A. Route optimization requires the MN B to send a Binding Update to Node A in order to create an entry in its binding cache that maps the MNs home address to its current care-of-address. However, prior to sending the binding update, the Mobile Node must first execute a Return Routability Test:

- the Mobile Node B has to send a Home Test Init message via its Home Agent and

- a Care of Test Init message directly to its Correspondent Node A.

The Care of Test Init message is sent using the new CoA of B as the source address. Such a packet does not match any entry in the firewall protecting A and as described in Section 2, the CoTi message will thus be dropped by the firewall. As a consequence, the RRT cannot be completed and route optimization cannot be applied. Every packet has to go through the node B's Home Agent and tunneled between B's Home Agent and B.

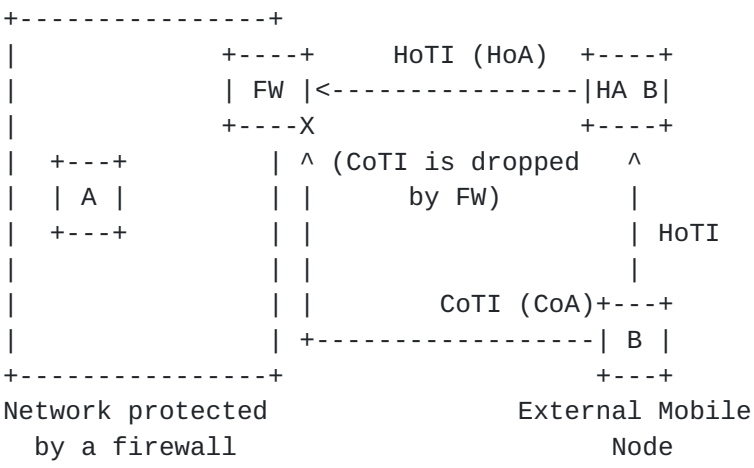

Figure 3. Issues with Return Routability Test

3.1.2 Issues with Firewall Status Update

Even if firewalls are made MIPv6 aware (which might require a different Binding Update security solution) a firewall might still drop packets coming from the new CoA since these incoming packets do not match any existing entry.

The packet filters in the firewall need to be updated with the COA of the MN in addition to its HoA.

Requiring the stateful inspection filters to update the connection state upon detecting Binding Update messages from a node outside the network protected by the firewall does not appear feasible nor desirable, since currently the firewall does not have any means to verify the validity of Binding Update messages and to therefore securely modify the state information. Changing the firewall states without verifying the validity of the Binding Update messages could lead to denial of service attacks. Malicious nodes may send faked Binding Update forcing the firewall to change its state information, and therefore leading the firewall to drop packets from the connections that use the legitimate addresses. An adversary might also use an address update to enable its own traffic to enter the network.

3.2 Scenario when the inner node is a Mobile Node

Let's assume a communication between an internal Mobile Node A, protected by a firewall, and an external node B. B can also be a Mobile Node protected by a firewall and issues raised in Section 3 apply in such case.

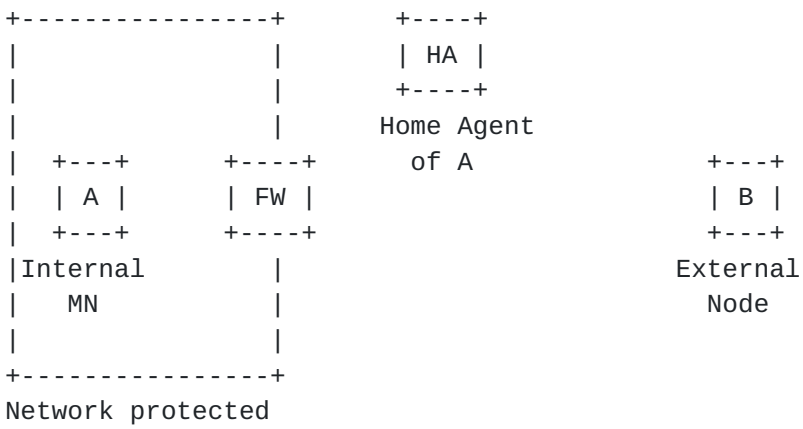

Figure 4. Issues between MIP6 and firewalls
when a firewall is protecting the MN

3.2.1 Issues with Binding Updates and Acknowledgements between the Mobile Nodes and their Home Agent

As required by [MIP6], the Mobile Node and the Home Agent MUST use IPsec to protect the integrity and authenticity of the Binding Updates and Acknowledgements. Both the Mobile Nodes and the Home Agents SHOULD use the Encapsulating Security Payload (ESP).

Many firewalls would however drop ESP packets (default behavior). This may cause the Binding Updates and Acknowledgements between the Mobile Nodes and their Home Agent to be dropped.

3.2.2 Issues with Reachability

One of the main advantages of Mobile IPv6 is that it allows the Mobile Node to be always reachable thanks to the Home Agent. A node desiring to establish a communication will send a packet to the Home Address of the MN which causes the packet to be routed to the home link of the MN. The Home agent intercepts the packet destined for the MN and forwards it to the MNs current point of attachment which is indicated by its care-of-address.

When considering firewalls, (e.g. when the Mobile Node roams to a network protected by a firewall), the packet forwarded from the Home Agent to the Mobile Node CoA may be dropped at the firewall since it does not match any existing entry. The following further describes the problem that might occur:

When entering the visited network, the MN first acquires a Care of Address and then sends a Binding Update to its Home Agent. This message creates a state in the firewall:

- it may be a state for the IPsec packet (in the case, the Binding Update message is protected by IPsec)

- or it may be a state for a mobility header in case IPsec is not used, but the security of the Binding Update is being provided by some other means such as an authentication option as specified in [AUTH] to solve the issue described in Section 4.1

The Binding Acknowledgement response can pass the firewall due to the created state, and be delivered to the Mobile Node.

Some firewalls may leave the created state open for a while (implementation dependent), whereas other firewalls may delete the state upon receiving the Binding Acknowledgement message.

Let's assume a Correspondent Node tries to initiate a communication with a Mobile Node. The Correspondent Node sends a packet to the Mobile Node's home address. The packet is intercepted by the MN's Home Agent which tunnels it to the MN's CoA.

As described in Section 2, the lifetime corresponding to the state in the firewall may have been expired and the state may have been removed. In such case, the incoming packet sent from the CN does not match any existing entry and is therefore dropped at the firewall.

Even if the state created above has not expired yet, the state created is for the Binding Update message (IPsec or Mobility Header) whereas the packet sent from the CN is received under the form of an IP in IP packet. The latter does not match any existing entry and is also dropped.

3.2.3 Return Routability Test

Security of Mobile IPv6 Binding Update between the MN and the CN is based on the RRT mechanism, the routing infrastructure and secret sharing (see [MIP6]). Since some RRT messages are routed via the home network, the strong trust relationship between the mobile node and the home agent (and the usage of IPsec ESP) is important. As specified in Mobile IPv6 [MIP6] in Section 5.2.5:

"For improved security, the data passed between the Home Agent and the Mobile Node is made immune to inspection and passive attacks. Such protection is gained by encrypting the home keygen token as it is tunneled from the Home Agent to the Mobile Node as specified in Section 10.4.6."

Section 10.4.6 furthermore specifies:

"The return routability procedure described in Section 5.2.5 assumes that the confidentiality of the Home Test Init and Home Test messages is protected as they are tunneled between the Home Agent to the Mobile Node. Therefore, the Home Agent MUST support tunnel mode IPsec ESP for the protection of packets belonging to the return routability procedure.".

This assumption is valid in some environments, however for networks protected by a firewall, the requirement can be an issue.

Typically firewalls need to filter the packets based on the source/destination IP addresses and the TCP/UDP source/destination ports numbers. When a packet is encrypted using IPsec ESP, such information is not available (in particular the port numbers), therefore firewalls may drop the Home Test messages forwarded by the HA to the MNs CoA. The result is that the MN cannot complete the RRT procedure, and consequently cannot perform route optimization by sending any Binding Update messages.

When ESP is applied, the firewall cannot differentiate packets containing the Mobility Header defined by MIPv6, i.e., packets for which Mobile IPv6 is used, from other packets. In order to support RRT, one possible idea could be to let the firewall pass all ESP packets coming from the MNs Home Agent. This may, however, not be desirable since it would allow several types of attacks (e.g. flooding) to be carried out against the MN. In cellular networks such flooding may result in attacks such as overbilling since the user is required to pay for all air-interface utilization.

A common approach, which is also used for NAT traversal, is to apply UDP encapsulation of IPsec packets. Unlike with NAT traversal it is not possible to detect the presence of a Firewall automatically in the same fashion as with a NAT. A NAT modifies the source IP address when an IP packet travels from the private to the public addressing space. For a Firewall this is not true. Hence, UDP encapsulation needs to be enabled proactively.

The Mobile Node would have to send UDP packets to the Home Agent to create the corresponding necessary state in the firewall. The Home Agent should also encapsulate the HoT message in a UDP datagram.

As other possible solutions, the home keygen token could be encrypted not using IPsec ESP but specific MIP6 fields within the HoT message so that the packet still appears as a Mobility Header one to the firewall as specified in [AUTH].

3.2.4 Issues with Change of CoA

The internal node A may change its CoA within the network which is protected by a firewall. Node A updates its mobility binding at the Home Agent by sending a Binding Update. Node A may also send Binding Update to its correspondent nodes.

However, even if firewalls are made MIPv6 aware to address the issues described in sections 4.1, 4.2 and 4.3, a firewall might still drop incoming packets sent to the new CoA since these incoming packets do not match any existing entry.

The packet filters in the firewall needs to be updated with the new COA of the MN.

3.2.5 Change of firewall

When the MN A moves, it may move to a link that is served by a different firewall. Node A might be sending BU to its CN, however incoming packets may be dropped at the firewall since the firewall on the new link that the MN attaches to does not have any state that is associated with the MN.

4. Conclusion

Current firewalls may not only prevent route optimization but may also prevent communications to be established in some cases. This document describes some of the issues between the Mobile IP protocol and current firewall technologies.

This document captures the various issues involved in the deployment of Mobile IPv6 in networks that would invariably include firewalls. A number of different scenarios are described which include configurations where the mobile node, correspondent node and home agent exist across various boundaries delimited by the firewalls. This enables a better understanding of the issues when deploying Mobile IPv6 as well as providing an understanding for firewall design and policies to be installed therein.

5. Security Considerations

This document describes several issues that exist between the Mobile IPv6 protocol and firewalls.

Firewalls may prevent Mobile IP6 traffic and drop incoming/outgoing traffic.

If the firewall configuration is modified in order to support the Mobile IPv6 protocol but not properly configured, many attacks may be possible as outlined above: malicious nodes may be able to

launch different types of denial of service attacks.

6. References

[3GPP] X. Chen, M. Watson, J. Wiljakka and J. Rinne Problem Statement for MIPv6 Interactions with GPRS/UMTS Packet Filtering IETF internet draft <draft-chen-mip6-gprs-01.txt>, July 2004

[AUTH] A. Patel, K. Leung, M. Khalil, H. Akhtar and K. Chowdhury, Authentication Protocol for Mobile IPv6, IETF internet draft <draft-patel-mipv6-auth-protocol-01.txt>, May 24, 2004

[CHES] William R. Cheswick and Steve M. Bellovin Firewalls and Internet Security, Repelling the Wily Hacker

[MIP6] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004

[STUN] Rosenberg, J., Weinberger, J., Huitema, C. and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

8. Author's Addresses:

Franck Le
Nokia Research Center, Dallas
6000 Connection Drive
Irving, TX-75039, USA.

E-Mail: franck.le@nokia.com
Phone : +1 972 374 1256

Stefano Faccin
Nokia Research Center, Dallas
6000 Connection Drive
Irving, TX-75039. USA.

E-Mail: stefano.faccin@nokia.com
Phone : +1 972 894 4994

Basavaraj Patil
Nokia, Dallas
6000 Connection Drive
Irving, TX-75039, USA.

EMail: Basavaraj.Patil@nokia.com
Phone: +1 972-894-6709

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: Hannes.Tschofenig@siemens.com

9. IPR Statement