MIP4 Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 22, 2007

M. Sahasrabudhe
Nokia
V. Devarapalli
Azaire Networks

October 19, 2006

Optimizations to Secure Connectivity and Mobility
draft-meghana-mip4-mobike-optimizations-01

Status of this Memo

Copyright Notice

Abstract

Users that need to connect to their enterprise network from an untrusted network require secure connectivity and mobility. Enterprise users are increasingly using mobile nodes. A user may need to connect to the enterprise network from anywhere, and in a number of scenarios, from untrusted networks. There are existing specifications developed by the Mobile IPv4 working group that describe solutions for enterprise secure connectivity and mobility.

This document proposes optimizations to those solutions to reduce the tunneling overhead and allow for a number of new access modes.

Table of Contents

1. Introduction

It is assumed that the reader is familiar with the use of MIP4 and MOBIKE to provide security connectivity and mobility to an enterprise user [2]. This document talks about optimizations to the solution proposed in [2] and also to [6]. An enterprise user authenticates to the VPN gateway from an untrusted network to gain access to the services on the enterprise network. While inside the network, a user doesn't need to use the VPN gateway. When a user roams in and out from a trusted to an untrusted network the sessions currently active should not drop and the change in connectivity should be seamless to the user.

The solution in [2] elaborates that the user uses only Mobile IPv4 [3] when inside the enterprise network and uses IPsec VPNs with MOBIKE extensions to IKEv2 when roaming outside the enterprise network to have access to the services provided by the enterprise. Point to note is that this solution does not support legacy IPsec VPNs. The VPN gateways have to implement mobility extensions to IKEv2 [4]. The solution also does not require multiple Home Agents or a Home Agent in the DMZ. The Home Agent is always located inside the enterprise network. The tunnel inner address of the IPsec tunnel is used as the MIPv4 co-located care of address (CCoA). As long as the mobile node is connected to the same VPN gateway and its TIA remains the same, there is no change in the CoA used by the mobile node. When the mobile node moves to a new VPN gateway or gets a new TIA, it updates its home agent with its new CCoA.

The packet format for packets sent from the mobile node to a correspondent node, when the mobile node is outside the enterprise, looks as follows

```
IPv4 hdr (src=IPA, dst=VPN_GW)
ESP Hdr
IPv4 hdr (src=TIA, dst=HA)
IPv4 hdr (src=HoA, dst=CN)
Payload
```

From the VPN gateway to the correspondent node the packet looks as follows

```
IPv4 hdr (src=TIA, dst=HA)
IPv4 hdr (src=HoA, dst=CN)
Payload
```

When the mobile node is inside the enterprise the packet format looks as follows

```
IPv4 hdr (src=IPA, dst=HA)
IPv4 hdr (src=HoA, dst=CN)
Payload
```

There is additional tunneling overhead when the mobile node is roaming in an untrusted network. This overhead can be avoided by having the Mobile IPv4 Foreign Agent functionality on the VPN gateway. This would avoid having to encapsulate a Mobile IP tunnel inside an IPsec tunnel. The following sections describe an optimized connectivity and roaming solution that reduces the packet overhead from the solution described in [2].

2. Terminology

i-MIP: Mobile IP layer used for internal enterprise mobility. Home Agent is inside the enterprise network.

x-MIP: Mobile IP layer used for access from outside the enterprise network. Home Agent resides either in the Internet or in the DMZ before the VPN gateway looking from the Internet

i-HA: Home Agent inside the enterprise network

x-HA: Home Agent outside the enterprise network

i-FA: Mobile IPv4 foreign agent residing in the trusted enterprise network

FA CoA: Foreign Agent mode care of address

cCoA: co-located care of address

HoA: Home address

TIA: Tunnel Inner Address, the address given out to the mobile node by the VPN gateway during IKE setup

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 [1].

3. Solution Overview

The optimization proposed in this document places the Foreign Agent on the VPN gateway. This reduces the tunnel overhead as the additional tunneling from the TIA to the Home Agent is not required.

When the VPN gateway receives the packet from the mobile node, it removes the IPsec header and the FA functionality on the VPN GW encapsulates the original packet and sends it to the Home Agent inside the enterprise.

The packet format from the mobile node to the VPN gateway now looks as follows

```
IPv4 hdr (src=IPA, dst=VPN_GW/FA)
ESP hdr
IPv4 hdr (src=HoA, dst=CN)
Payload
```

From the VPN gateway to the correspondent node the packet looks as follows

```
IPv4 hdr (src=VPN_GW/FA, dst=HA)
IPv4 hdr (src=HoA, dst=CN)
Payload
```

Figure 6 depicts the network topology assumed for the solution. It also shows the possible mobile node locations and access modes.

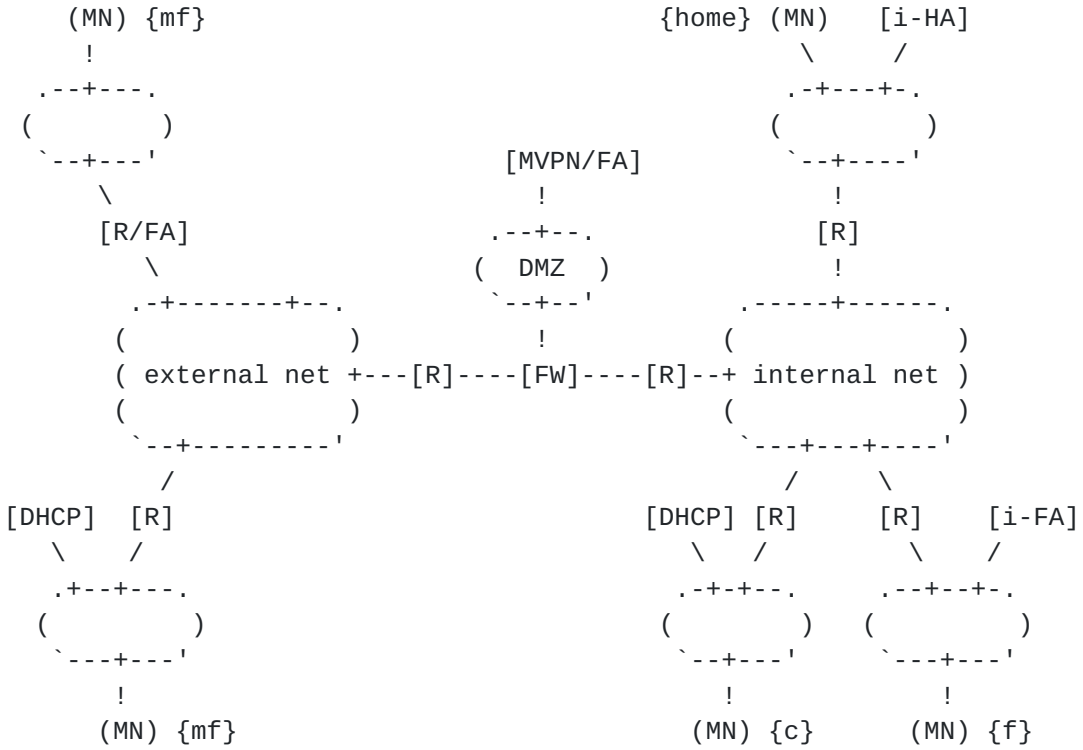

Figure 6: Network Topology with FA colocated on VPN gateway

The tunnel overhead reduction is significant especially if the mobile node is connected over a wireless network. The optimization requirement of co-locating the Foreign Agent with the VPN gateway can place the FA multiple hops away from the mobile node. FA availability is hence an issue here. The FA still has to be on link for the mobile node to receive Agent Advertisement messages. There already exists a tunnel interface between the mobile node and the VPN gateway. This tunnel interface can be used so the FA can appear just one hope away and on link to the mobile node. The FA sends out Agent Advertisement messages on the tunnel interface. The mobile node too can send out MIP control messages to the FA on the tunnel interface.

3.1. Access modes

The access modes possible in [1] are

f: i-MIP with FA-CoA
c: i-MIP with CCoA
mc: mobile enhanced VPN, i-MIP with VPN TIA as CCoA

The additional access modes possible with the optimizations in this document are

fvf: x-MIP with FA CoA/ VPN/ i-MIP with FA CoA
cvf: x-MIP with CCoA/VPN/ i-MIP with FA CoA
mf: mobile enhanced VPN, i-MIP with FA CoA

3.2. Access mode: 'fvf'

In this access mode there are two home agents. One Home Agent is located inside the enterprise and one outside the enterprise in the internet or the DMZ before the VPN gateway looking from the internet. In this mode the mobile node uses the external care-of address (x-FACoA) and an external home address (x-HoA). Packets are first tunneled to the external home Agent, then to the VPN gateway and eventually to the internal home Agent.

Packet format from the mobile node to the VPN gateway looks as follows:

```
IPv4 hdr (src=x-FA-CoA, dst=x-HA)
IPv4 hdr (src=i-HoA, dst=VPN_GW/FA)
ESP hdr
IPv4 hdr (src=i-HoA, dst=CN)
Payload
```

Packet format from the VPN gateway to the correspondent node looks as follows:

```
IPv4 hdr (src=VPN_GW/FA, dst=i-HA)
IPv4 hdr (src=i-HoA, dst=CN)
Payload
```

3.3. Access mode: 'cvf'

There are two home agents here also. One Home Agent is located inside the enterprise and one outside the enterprise in the internet or the DMZ before the VPN gateway looking from the internet. In this mode tme mobile node uses the external co-located care-of address (x-cCoA) and an external home address (x-HoA).Packets are first tunneled to the external home Agent, then to the VPN gateway and eventually to the internal home Agent.

Packet format from the mobile node to the VPN gateway looks as follows:

```
IPv4 hdr (src=x-cCoA, dst=x-HA)
IPv4 hdr (src=i-HoA, dst=VPN_GW/FA)
ESP hdr
IPv4 hdr (src=i-HoA, dst=CN)
Payload
```

Packet format from the VPN gateway to the correspondent node looks as follows

```
IPv4 hdr (src=VPN_GW/FA, dst=i-HA)
IPv4 hdr (src=i-HoA, dst=CN)
Payload
```

3.4. Access mode: 'mf'

In this mode the VPN gateway is mobility aware in the sense that it also implements MOBIKE extensions in addition to being a Foreign Agent. The mobile node uses the TIA as a co-located care-of address.

Packet format from mobile node to the VPN GW/FA looks as follows:

```
IPv4 hdr (src=IPA, dst=VPN_GW/FA)
ESP hdr
IPv4 hdr (src=TIA, dst=HA)
IPv4 hdr (src=HoA, dst=CN)
Payload
```

Packet format from the VPN gateway to the correspondent node looks as follows:

```
IPv4 hdr (TIA, dst=i-HA)
IPv4 hdr (src=i-HoA, dst=CN)
Payload
```

The advantage in using access modes 1 and 2 is that these can still be used with legacy IPsec VPNs. Hence these can be deployed in existing enterprise networks that may have already invested heavily in legacy VPNs and would be reluctant to upgrade the VPN gateways in the enterprise network.

4. Home Address as IPsec TIA

When the mobile node sets up an IPsec tunnel with the VPN gateway it is allocated a tunnel inner address (TIA). The TIA is used as the source address for all traffic sent through the IPsec tunnel. The tunnel mode IPsec security associations are created based on TIA. But when a foreign agent functionality exists on the VPN gateway, the mobile node MUST use the home address as the source address on the data traffic. Moreover, the optimization described in Section 3.4 is possible only if the home address is equal to the TIA.

In order for the home address to be equal to the TIA, there is a need for close interaction between the IKEv2 implementation and Foreign agent implementation on the VPN gateway. This may not be possible with all implementations, since the IPsec tunnel setup happens before an Foreign Agent Advertisement can be sent over the IPsec tunnel to the mobile node. One possible solution would be to allocate a TIA when the IPsec tunnel is setup and later replace the TIA with the home address. This would require updating the IPsec SAs with the new home address. But this would violate RFC 4301 [8] which says the TIA cannot be changed without rendering the tunnel mode IPsec SAs invalid.

A simple solution would be for the mobile node to setup an IPsec tunnel with the TIA allocated by the VPN gateway, and then run a separate CREATE_CHILD_SA exchange [5] to setup new tunnel mode IPsec security associations for the home address. This would however introduce additional delay in the form of an additional CREATE_CHILD_SA exchange when the mobile node connects to the enterprise network from outside. The security associations created earlier for the TIA may be either torn down or allowed to expire based on the configuration on the mobile node and the VPN gateway.

5. Security Considerations

The solution described in this document does not introduce any new

security vulnerabilities on top of what is described in the security considerations sections of [2], [6] and [7].

6. IANA Considerations

This document requires no action from IANA.

7. References

7.1. Normative References

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

[2] Devarapalli, V. and P. Eronen, "Secure Connectivity and Mobility using Mobile IPv4 and MOBIKE", draft-ietf-mip4-mobike-connectivity-01 (work in progress), June 2006.

[3] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[4] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[5] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

7.2. Informative References

[6] Vaarala, S. and E. Klovning, "Mobile IPv4 Traversal Across IPsec-based VPN Gateways", draft-ietf-mip4-vpn-problem-solution-02 (work in progress), November 2005.

[7] Adrangi, F. and H. Levkowetz, "Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways", RFC 4093, August 2005.

[8] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

Authors' Addresses

Meghana Sahasrabudhe
Nokia
313 Fairchild Drive
Mountain View, CA 94043
USA

Email: meghana.saha@nokia.com

Vijay Devarapalli
Azaire Networks
4800 Great America Parkway
Santa Clara, CA 95054
USA

Email: vijay.devarapalli@azairenet.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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