MIP4 Working Group V. Devarapalli
Internet-Draft P. Eronen
Expires: July 26, 2006 Nokia
January 22, 2006

Secure Connectivity and Mobility using Mobile IPv4 and MOBIKE
draft-ietf-mip4-mobike-connectivity-00

Status of this Memo

Copyright Notice

Abstract

Enterprise users require mobility and secure connectivity when they roam and connect to the services offered in the enterprise. Secure connectivity is required when the user connects to the enterprise from an untrusted network. Mobility is beneficial when the user moves, either inside or outside the enterprise network, and acquires a new IP address. This document describes a solution using Mobile IPv4 and mobility extensions to IKEv2 (MOBIKE) to provide secure connectivity and mobility.

Table of Contents

1. Introduction 3
2. Terminology 4
3. Solution Overview 5
3.1. Access modes 6
3.1.1. Access mode: 'c' 6
3.1.2. Access mode: 'f' 6
3.1.3. Access mode: 'mc' 7
3.2. Mobility within the enterprise 7
3.3. Mobility when outside the enterprise 7
3.4. Crossing Security Boundaries 8
3.4.1. Operation when moving from an untrusted network . . . 8
3.4.2. Operation when moving from a trusted network 9
4. NAT Traversal 9
5. Security Considerations 10
6. IANA Considerations 10
7. Acknowledgments 10
8. References 10
8.1. Normative References 10
8.2. Informative References 11
Authors' Addresses 12
Intellectual Property and Copyright Statements 13

1. Introduction

A typical enterprise network consists of users connecting to the services from a trusted network (intranet), and from an untrusted network (Internet). The trusted and untrusted networks are typically separated by a demilitarized zone (DMZ). Access to the intranet is controlled by a firewall and a VPN gateway in the DMZ.

Enterprise users, when roaming on untrusted networks, most often have to authenticate themselves to the VPN gateway and set up a secure tunnel in order to access the intranet. The use of IPsec VPNs is very common to enable such secure connectivity to the intranet. When the user is on the trusted network, VPNs are not used. However, the users benefit tremendously when session mobility between subnets, through the use of Mobile IPv4, is available.

There has been some work done on using Mobile IPv4 and IPsec VPNs to provide roaming and secure connectivity to an enterprise [10]. The solution described in [10] was designed with certain restrictions, including requiring no modifications to the VPN gateways and involves the use of two layers of MIPv4, with one home agent inside the intranet and one in the Internet or in the DMZ before the VPN gateway. The per-packet overhead is very high in this solution. It is also challenging to implement and have two instances of MIPv4 active at the same time on a mobile node. However, the solution described here is only applicable when IKEv2 IPsec VPNs are used.

This document describes an alternate solution that does not require two layers of MIPv4. The solution described in this document uses Mobile IPv4 when the mobile node is on the trusted network and MOBIKE capable IPsec VPNs when mobile node is on the untrusted network. The mobile node uses the tunnel inner address (TIA) given out by the IPsec VPN gateway as the co-located CoA for MIPv4 registration. This eliminates the need for using an external MIPv4 home agent and the need for encapsulating the VPN tunnel inside a MIPv4 tunnel.

The following assumptions are made for the solution described in this document.

- IKEv2 [4] and IPsec [5] are used to set up the VPN tunnels between the mobile node and the VPN gateway.
- The VPN gateway and the mobile node support MOBIKE extensions as defined in [3].
- When the mobile node is on the trusted network, traffic should not go through the DMZ. Current deployments of firewalls and DMZs consider the scenario where only a small amount of the total enterprise traffic goes through the DMZ. Routing through the DMZ typically involves stateful inspection of each packet by the

firewalls in the DMZ.

- When the mobile node is on the trusted network and uses a wireless access technology, confidentiality protection of the data traffic is provided by the particular access technology. In some networks, confidentiality protection MAY be available between the mobile node and the first hop access router, in which case it is not required at layer 2.

Mobility extensions for IKEv2 are being standardized. There is no similar effort for IKEv1 [6].

This document also presents a solution for the mobile node to detect when it is on a trusted network, so that the IPsec tunnel can be dropped and the mobile node can use Mobile IP in the intranet.

2. Terminology

Many of the following terms are defined in [10], but are repeated here to make this document self-contained.

FA: Mobile IPv4 foreign agent

CCoA: co-located Care-of address

FA-CoA: Foreign Agent Care-of address

FW: Firewall

i-FA: Mobile IPv4 foreign agent residing in the trusted (intranet) network

i-HA: Mobile IPv4 home agent residing in the trusted (intranet) network

i-MIP: The mobile node uses the home agent in the internal network

VPN TIA: VPN tunnel inner address. This address is given out by the VPN gateway during IKE negotiation and is routable in the trusted network

mVPN: VPN with MOBIKE functionality

The following access modes are used in explaining the protocol. The access modes are explained in more detail in [10].

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

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 mobile node is configured with a home address that remains the same irrespective of whether the mobile node is inside or outside the enterprise network. The mobile node is also reachable at the same home address irrespective of its current point of attachment. When the mobile node is connected to the intranet directly, it uses Mobile IP for internal mobility.

When the mobile node roams and connects to an untrusted network outside the enterprise, it sets up a VPN tunnel to the VPN gateway. However, it still maintains a valid binding cache entry at the i-HA. It uses the VPN TIA, allocated by the VPN gateway, as the co-located CoA for registration with the i-HA. If the VPN TIA changes or if the mobile node moves and connects to another VPN gateway, then it sends a Registration Request to the i-HA using the new co-located CoA.

If the mobile node moves while outside the enterprise and its access network changes, it uses the MOBIKE protocol to update the VPN gateway of its current address. The internal home agent is not aware of the mobile node's movement as long as the mobile node is attached to the same VPN gateway and the TIA remains the same.

Figure 1 depicts the network topology assumed for the solution. It also shows the possible mobile node locations and access modes.

```
       (MN) {mc}                             {home} (MN)   [i-HA]
        !                                             \     /
     .--+---.                                        .-+---+-.
    (        )                                      (         )
     `--+---'                      [MVPN]            `--+----'
         \                           !                  !
         [R/FA]                   .--+--.              [R]
            \                    (  DMZ  )              !
           .-+-------+--.         `--+--'         .-----+------.
          (              )           !           (              )
          ( external net +---[R]----[FW]----[R]--+ internal net )
          (              )                       (              )
           `--+---------'                         `---+---+----'
             /                                       /     \
   [DHCP]  [R]                              [DHCP] [R]     [R]    [i-FA]
      \    /                                   \   /         \    /
      .+--+---.                               .-+-+--.     .--+--+-.
     (         )                             (        )   (         )
      `---+---'                               `--+---'     `---+---'
          !                                      !             !
         (MN) {mc}                             (MN) {c}      (MN) {f}
```

Figure 1: Network Toplogy using MIPv4 and MOBIKE

The solution described above results in a Mobile IP tunnel inside an IPsec tunnel. The Mobile IP tunnel is between the mobile node and the home agent and the IPsec tunnel is between the MN and the mVPN gateway. The Mobile IP tunnel uses reverse tunneling through the home agent [12].

3.1. Access modes

The following access modes are used in the solution described in this document.

3.1.1. Access mode: 'c'

This access mode is standard Mobile IPv4 [2] with a co-located care-of address. The mobile node must detect that it is connected to an internal trusted network before using this mode. The co-located care-of address is assigned by the access network to which the mobile node is attached to.

3.1.2. Access mode: 'f'

This access mode is standard Mobile IPv4 [2] with a foreign agent care-of address. The mobile node can use this mode only when it detects that it is connected to an internal trusted network and also

detects a foreign agent on the access network.

3.1.3. Access mode: 'mc'

This access mode involves using both Mobile IPv4 and a MOBIKE enabled IPsec VPN gateway, resulting in a Mobile IP tunnel inside an IPsec tunnel. The mobile node uses the VPN TIA as the co-located CoA for registering with the home agent. This mode is used only when the mobile node is attached to an untrusted network and is required to set up an IPsec tunnel with a VPN gateway to gain access to the trusted network.

3.2. Mobility within the enterprise

When the mobile node is inside the enterprise network and attached to the intranet, it uses Mobile IPv4 [2] for subnet mobility. The mobile node uses a foreign agent care-of address, if a foreign agent is available. Otherwise it acquires an address through DHCP on the access link and uses it as the co-located care-of address for Mobile IP. The mobile node attempts Foreign Agent discovery and CoA address acquisition through DHCP simultaneously in order to avoid the delay in discovering a foreign agent when there is no foreign agent available. The mobile node maintains a valid binding cache entry at all times at the home agent mapping the the home address to the current CoA. Whenever the mobile node moves, it sends a Registration Request to update the binding cache entry.

The Mobile IP signaling messages between the mobile node and the home agent are authenticated as described in [2].

The mobile node maintains a valid binding cache entry at the home agent even when it is outside the enterprise network.

3.3. Mobility when outside the enterprise

When the mobile node is attached to an untrusted network, it sets up an IPsec VPN tunnel with the VPN gateway to gain access to the enterprise network. If the mobile node moves and its IP address changes, it initiates the MOBIKE protocol [3] to update the address on the VPN gateway.

The mobile node maintains a binding at the home agent even when it is outside the enterprise network. If the TIA changes or the mobile node attaches to another VPN gateway, the mobile node should send a Registration Request to its home agent to update the binding cache with the new TIA.

3.4. Crossing Security Boundaries

Security boundary detection is based on the reachability of the i-HA from the mobile node's current point of attachment. Whenever the mobile node detects that it has moved to a new IP subnet [13] and its IP address changes, it sends a Registration Request to the i-HA without any VPN encapsulation. If the mobile node receives a Registration Reply, then it is assumes that it is on a trusted network. This is based on the mechanism described in [10] to detect attachment to the internal trusted network. The mobile node should re-transmit the Registration Request if it does not receive the Registration Reply within a timeout period. The number of times the mobile node should re-transmit the Registration Request and the timeout period for receiving the Registration Reply are configurable on the mobile node.

If the mobile node has an existing VPN tunnel to its VPN gateway, it MUST send a MOBIKE message at the same time as the registration request to the i-HA whenever the IP address changes. If the mobile node receives a response from the VPN gateway, but not from the i-HA, it assumes it is outside the enterprise network. If it receives a response from the i-HA, then it assumes it is inside the enterprise network.

There could also be some out-of-band mechanisms that involve configuring the wireless access points with some information which the mobile node can recognize as access points that belong to the trusted network in an enterprise network. Such mechanisms are beyond the scope of this document.

3.4.1. Operation when moving from an untrusted network

When the mobile node is outside the enterprise network and attached to an untrusted network, it has an IPsec VPN tunnel with its mobility aware VPN gateway, and a valid registration with a home agent on the intranet with the VPN TIA as the care-of address.

If the mobile nodes moves and its IP address changes, it performs the following steps:

1a. Initiate an IKE mobility exchange to update the VPN gateway with the current address. If the new network is also untrusted, this will be enough for setting up the connectivity. If the new network is trusted, and if the VPN gateway is reachable, this exchange will allow the mobile node to keep the VPN state alive while on the trusted side. If the VPN gateway is not reachable from inside, then this exchange will fail.

1b. At the same time as step 1, send a Mobile IPv4 Registration Request to the internal home agent without VPN encapsulation.

2. If the mobile node receives a Registration Reply to the request sent in step 2, then the current subnet is a trusted subnet, and the mobile node can communicate without VPN tunneling. The mobile node MAY tear down the VPN tunnel.

3.4.2. Operation when moving from a trusted network

When the mobile node is inside the enterprise and attached to the intranet, it does not use a VPN tunnel for data traffic. It has a valid binding cache entry at its home agent. If the VPN gateway is reachable from the trusted network, the mobile node MAY have valid IKEv2 security associations with its VPN gateway. The IPsec security associations can be created when required. The mobile node may have to re-negotiate the IKEv2 security associations to prevent them from expiring.

If the mobile node moves and its IP address changes, it performs the following steps:

1. Initiate an IKE mobility exchange to update the VPN gateway with the current address, or if there is no VPN connection, then establish a VPN tunnel with the gateway from the new local IP address. If the new network is trusted, and if the VPN gateway is reachable, this exchange will allow the mobile node to keep the VPN state alive, while in the trusted side. If the new network is trusted and if the VPN gateway is not reachable from inside, then this exchange will fail.
2. At the same time as step 1, send a Mobile IPv4 Registration Request to the internal home agent without VPN encapsulation.
3. If the mobile node receives a Registration Reply to the request sent in step 2, then the current subnet is a trusted subnet, and the mobile node can communicate without VPN tunneling, using only Mobile IP with the new care-of address.
4. If the mobile node didn't receive the response in step 3, and if the VPN tunnel is successfully established and registered in step 1, then the mobile node sends a Registration Request over the VPN tunnel to the internal home agent. After receiving a Registration Reply from the home agent, the mobile node can start communicating over the VPN tunnel with the Mobile IP home address.

4. NAT Traversal

There could be a NAT device between the mobile node and the home agent in any of the access modes, 'c', 'f' and 'mc', and between the

mobile node and the VPN gateway in the access mode 'mc'. Mobile IPv4 NAT traversal, as described in [7] should be used by the mobile node and the home agent in access modes 'c' or 'f', when there is a NAT device present. When using access mode, 'mc', IPsec NAT traversal [8] [9] should be used by the mobile node and the VPN gateway, if there is a NAT device present. Typically, the TIA would be a routable address inside the enterprise network. But in some cases, the TIA could be from a private address space associated with the VPN gateway. In such a case, Mobile IPv4 NAT traversal should be used in addition to IPsec NAT traversal in the 'mc' mode.

5. Security Considerations

Enterprise connectivity typically requires very strong security, and the solution described in this document was designed keeping this in mind.

Security concerns related to the mobile node detecting that it is on a trusted network and thereafter dropping the VPN tunnel are described in [10].

Please see [3] for MOBIKE-related security considerations, and [7], [8] for security concerns related to the use of NAT traversal mechanisms for Mobile IPv4 and IPsec.

6. IANA Considerations

This document requires no action from IANA.

7. Acknowledgments

The authors would like to thank Henry Haverinen, Sandro Grech, Dhaval Shah and John Cruz for their participation in developing this solution.

The authors would also like to thank Henrik Levkowetz, Jari Arkko and TJ Kniveton for reviewing the document.

8. References

8.1. Normative References

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

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

[3] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", draft-ietf-mobike-protocol-07 (work in progress), December 2005.

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

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

[6] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[7] Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, May 2003.

[8] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[9] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[10] 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.

8.2. Informative References

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

[12] Montenegro, G., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[13] Aboba, B., "Detecting Network Attachment in IPv4 (DNAv4)", draft-ietf-dhc-dna-ipv4-18 (work in progress), December 2005.

Authors' Addresses

Vijay Devarapalli
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94043
USA

Email: vijay.devarapalli@nokia.com

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland

Email: pasi.eronen@nokia.com

Intellectual Property Statement

Disclaimer of Validity

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 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.

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.