Network Working Group
Request for Comments: 5266
BCP: 136
Category: Best Current Practice

V. Devarapalli
Wichorus
P. Eronen
Nokia

June 2008

Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE)

Status of This Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

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 (MIPv4) and mobility extensions to IKEv2 (MOBIKE) to provide secure connectivity and mobility.

Table of Contents

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 Virtual Private Network (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 [RFC5265] [RFC4093]. The solution described in [RFC5265] 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 Internet Key Exchange Protocol version 2 (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 the 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 care-of address (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 [RFC4306] and IPsec [RFC4301] 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 [RFC4555].

- 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. Moreover, the DMZ architecture assumes that the DMZ is less secure than the internal network. Therefore, the DMZ-based architecture allows the least amount of traffic to traverse the DMZ, that is, only traffic between the trusted network and the external network. Requiring all normal traffic to the mobile nodes to traverse the DMZ would negate this architecture.

- 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.

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.

IPsec VPN gateways that use IKEv1 [RFC2409] are not addressed in this document.

2. Terminology

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].

Many of the following terms are defined in [RFC5265], but are repeated here to make this document self-contained.

FA: Mobile IPv4 foreign agent.

Co-CoA: 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 [RFC5265].

f: i-MIP with FA-CoA

c: i-MIP with Co-CoA

mc: i-MIP with MOBIKE-enabled VPN, with VPN-TIA as Co-CoA

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.

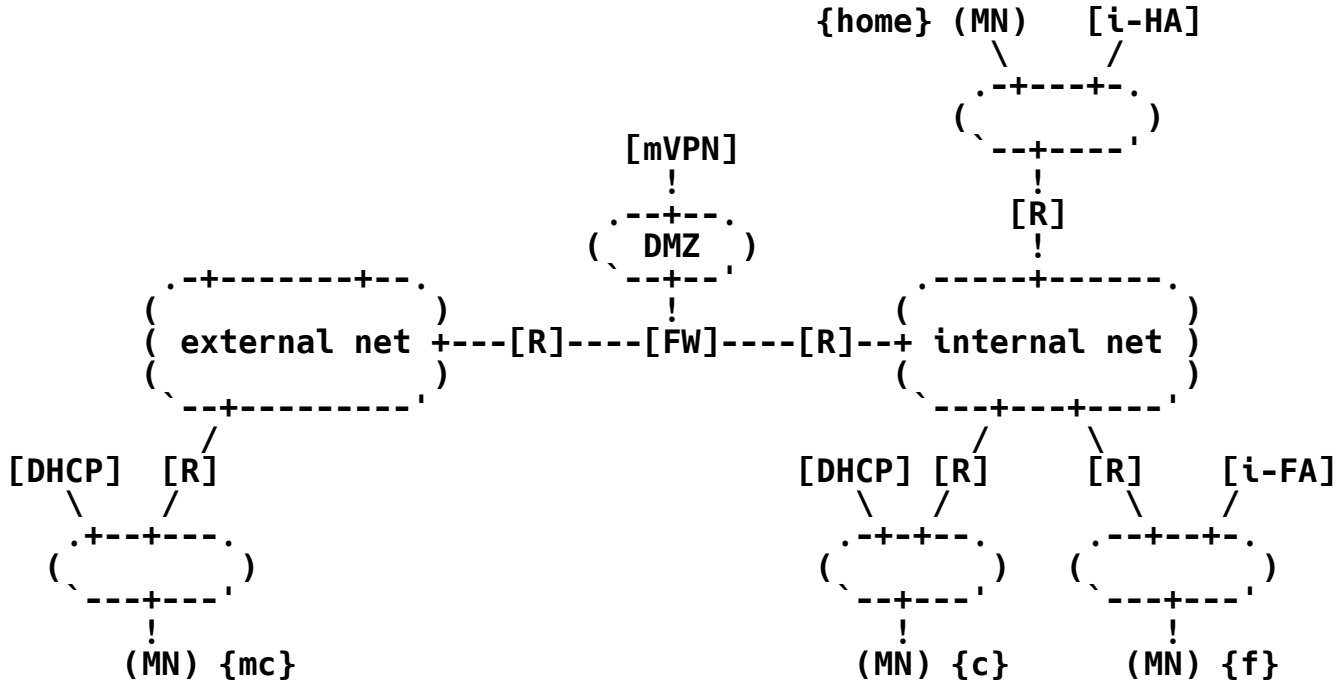

Figure 1: Network Topology Using MIPv4 and MOBIKE

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 mobile node (MN) and the mVPN gateway. The mobile node MUST reverse tunnel through the home agent [RFC3024] when the Mobile IP tunnel is inside an IPsec tunnel.

The overhead of running a Mobile IP tunnel inside an IPsec tunnel can be avoided by having the Mobile IP foreign agent functionality on the VPN gateway. This is out of scope for this document and is further described in [MEGHANA].

Whenever the mobile node attaches to a new link, it may encounter a foreign agent. The mobile node MUST not use the foreign agent care-of address with the i-HA when attached to an untrusted access network. The default behavior for the mobile node is to always configure an address from the access link using DHCP. The mobile node then checks if it is attached to a trusted access network by sending a Registration Request to the i-HA in the co-located care-of address mode. If the mobile node discovers that it is attached to a trusted access network, then it MAY start using a foreign agent care-of address with the i-HA. In order to do this, the mobile node has to perform a new registration with the i-HA.

The mobile node can use a foreign agent on a untrusted access network, if there is an external home agent that the mobile node is able to use. The use of an external home agent in the untrusted access network and a home agent in the trusted access network at the same time is described in detail in [RFC5265].

Some IPsec VPN implementations allow a host to send traffic directly to the Internet when attached to an untrusted network. This traffic bypasses the IPsec tunnel with the VPN gateway. This document does not prevent such traffic from being sent out from the host, but there will be no mobility or session continuity for the traffic. Any data traffic that is sent through the Mobile IP tunnel with the home agent is always sent through the VPN gateway.

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 [RFC3344] 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.

3.1.2. Access Mode: 'f'

This access mode is standard Mobile IPv4 [RFC3344] 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 [RFC3344] for subnet mobility. The mobile node always configures a care-of address through DHCP on the access link and uses it as the co-located care-of address. The mobile node MAY use a foreign agent care-of address, if a foreign agent is available. However, the foreign agent care-of address is used only when the mobile node is attached to the trusted access network. 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 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 [RFC3344].

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 [RFC4555] 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 due to the mobile node re-connecting to the VPN gateway or attaching to a different 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 a change in network connectivity, it sends a Registration Request to the i-HA without any VPN encapsulation. If the mobile node receives a Registration Reply with the Trusted Networks Configured (TNC) extension from the i-HA, then it assumes that it is on a trusted network. The TNC extension is described in [RFC5265]. The mobile node MUST check that the Registration Reply is integrity protected using the mobile node-home agent mobility

security association before concluding it is attached to a trusted network. This security boundary detection is based on the mechanism described in [RFC5265] 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.

When the mobile node is attached to an untrusted network and is using an IPsec VPN to the enterprise network, the ability to send a Registration Request to the i-HA without VPN encapsulation would require some interaction between the IPsec and MIPv4 modules on the mobile node. This is local to the mobile node and out of scope for this document.

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 that 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.

The mobile node should not send any normal traffic while it is trying to detect whether it is attached to the trusted or untrusted network. This is described in more detail in [RFC5265].

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 node 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 1b, 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 Network Address Translation (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 [RFC3519], 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 [RFC3947] [RFC3948] 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 [RFC5265].

When the mobile node sends a Registration Request to the i-HA from an untrusted network that does not go through the IPsec tunnel, it will reveal the i-HA's address, its own identity including the NAI and the home address, and the Authenticator value in the authentication extensions to the untrusted network. This may be a concern in some deployments.

Please see [RFC4555] for MOBIKE-related security considerations, and [RFC3519], [RFC3947] for security concerns related to the use of NAT traversal mechanisms for Mobile IPv4 and IPsec.

6. 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, TJ Kniveton, Vidya Narayanan, Yaron Sheffer, Hans Sjostrand, Jouni Korhonen, and Sami Vaarala for reviewing the document.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5265] Vaarala, S. and E. Klovning, "Mobile IPv4 Traversal across IPsec-Based VPN Gateways", RFC 5265, June 2008.

7.2. Informative References

[RFC4093] Adrangi, F. and H. Levkowetz, "Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways", RFC 4093, August 2005.

[RFC3024] Montenegro, G., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[MEGHANA] Sahasrabudhe, M. and V. Devarapalli, "Optimizations to Secure Connectivity and Mobility", Work in Progress, February 2008.

[RFC3519] Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, April 2003.

[RFC3947] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

Appendix A. Applicability to a Mobile Operator Network

The solution described in this document can also be applied to a Mobile Operator's network when the Operator deploys heterogeneous access networks and some of the access networks are considered as trusted networks and others as untrusted networks. Figure 2 illustrates such a network topology.

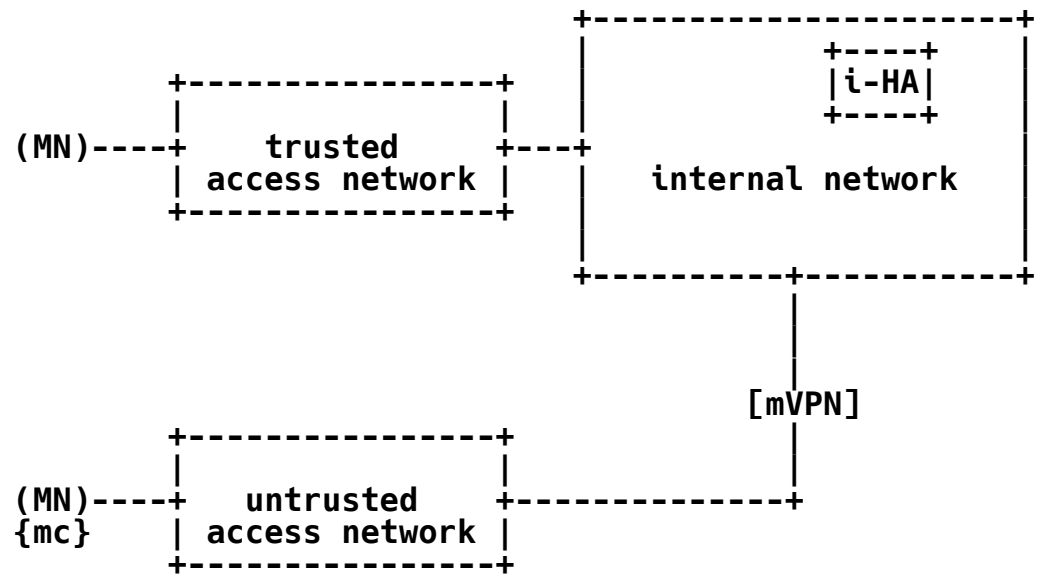

Figure 2: Network Topology of a Mobile Operator with Trusted and Untrusted Networks

An IPsec VPN gateway provides secure connectivity to the Operator's internal network for mobile nodes attached to an untrusted access network. The VPN gateway supports MOBIKE extensions so that the IPsec tunnels survive any IP address change when the mobile node moves while attached to the untrusted access networks.

When the mobile node is attached to the trusted access network, it uses Mobile IP with the i-HA. It uses the IP address obtained from the trusted access network as the co-located care-of address to register with the i-HA. If a foreign agent is available in the trusted access network, the mobile node may use a foreign agent care-of address. If the mobile node moves and attaches to an untrusted access network, it sets up an IPsec tunnel with the VPN gateway to access the Operator's internal network. It uses the IPsec TIA as the co-located care-of address to register with the i-HA thereby creating a Mobile IP tunnel inside an IPsec tunnel.

When the mobile node is attached to the trusted access network, it can either be attached to a foreign link in the trusted network or to the home link directly. This document does not impose any restrictions.

Authors' Addresses

Vijay Devarapalli
Wichorus
3590 North First Street
San Jose, CA 95134
USA

EMail: vijay@wichorus.com

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

EMail: pasi.eronen@nokia.com

Full Copyright Statement

Intellectual Property