Network Working Group
Internet-Draft
Expires: January 17, 2003

A. Nuopponen
S. Vaarala
Netseal
July 19, 2002

Mobile IPv4 coexistence with IPsec remote access tunnelling
draft-nuopponen-vaarala-mipvpn-00

Status of this Memo

Copyright Notice

Abstract

This document describes a simple method that allows a mobile node to use a home agent situated inside a protected intranet, while also allowing the mobile to roam between the public internet and the intranet without losing active sessions. Whenever the mobile is outside the intranet, it connects to the intranet using an IPsec tunnel and registers the IPsec-assigned inner tunnel address as its co-located care-of address to the internal home agent. If desired, handover performance while outside the intranet can be enhanced by employing another Mobile IP layer underneath IPsec. The solution does not require any new protocols, only a profile for using existing protocols. Only the mobile node needs to be modified in order to use

this profile.

Table of Contents

1. Introduction

In some deployment scenarios it is desireable to use Mobile IPv4 in a protected corporate intranet to provide mobility for users, while using a VPN device on the network edge to protect against unauthorized access. In such a deployment, it would be desireable for users to be able to roam from the intranet to the external network (and back) while maintaining active sessions.

Mobile IPv4 and VPN coexistence problem statement and solution requirements are described in [2]. This document describes a simple method for solving these coexistence problems by defining a profile for combining Mobile IPv4 and IPsec in a certain way.

2. Description of the solution

2.1 Network topology

The network topology assumed by the solution is described in this section. The description is described with regards to service rendered for a single mobile node.

The home network consists of the following components:

- the home agent providing service to the mobile node
- optional foreign agents
- optional site-to-site IPsec tunnels
- the intranet interface(s) of one or more IPsec devices (which are not necessarily in the home network, but in the trusted side of the device anyway)

The external network consists of the following components:

- the external interface(s) of one or more IPsec devices
- optional "trusted foreign agents" that are connected to the home network using a static IPsec tunnel, and are thus logically part of the intranet (see [2] for definition)
- optional external Mobile IP home agent used to optimize IPsec tunnel handover performance
- optional foreign agents to support the use of the abovementioned external home agent
- possibly NAT device(s) between (not all apply):
  - the mobile node and the IPsec device
  - a trusted foreign agent and the IPsec device
  - the mobile node and an external home agent
  - the external home agent and the IPsec device

The external network access alternatives are summarized in the following figure.

```
1a. mn ================================ vpn -- ha
1b. mn == nat ========================== vpn -- ha
1c. mn ++ t-fa ========================= vpn -- ha
1d. mn ++ t-fa == nat ================== vpn -- ha

2a. mn ################## e-ha ========= vpn -- ha
2b. mn ################## e-ha == nat == vpn -- ha
2c. mn ## nat ########## e-ha ========= vpn -- ha
2d. mn ## nat ########## e-ha == nat == vpn -- ha
2e. mn == e-fa ######### e-ha ========= vpn -- ha
2f. mn == e-fa ######### e-ha == nat == vpn -- ha
2g. mn == e-fa ## nat ## e-ha ========= vpn -- ha
2h. mn == e-fa ## nat ## e-ha == nat == vpn -- ha
```

Encapsulation markers:

--	unprotected, Mobile IP tunnelled (reverse tunnelling)
==	Mobile IP tunnelled, then IPsec protected
++	unprotected, plain packets (not Mobile IP tunnelled)
##	Mobile IP tunnelled, then IPsec protected, then (possibly) Mobile IP tunnelled again

Network elements:

mn	mobile node
vpn	IPsec edge device
ha	internal home agent
t-fa	trusted foreign agent (logically part of intranet)
e-ha	external home agent
e-fa	external foreign agent, used to communicate with the external home agent
nat	NAT device

2.2 Summary of solution

When the mobile node resides in the home network, Mobile IPv4 is applied normally.

Site-to-site IPsec tunnels work transparently: the mobile still uses standard Mobile IPv4, and the registration request/reply messages and data messages are tunneled normally between sites.

When outside the home network, the mobile node can be considered to be at the remote end of a site-to-site IPsec tunnel consisting only of a single address, the "inner" address of the IPsec tunnel. This address is either configured manually, or the IPsec-DHCP mechanism

can be leveraged [4].

The "inner" address of the IPsec tunnel is used as a co-located care-of address for a standard Mobile IPv4 registration. Because the routing in the intranet is organized in a way that ensures that packets destined to this care-of address are routed to the IPsec device, they will get tunnelled to the mobile node normally.

Because the mobile node never logically leaves the intranet, sessions survive mobility between the intranet and the external network.

Because IPsec is not mobile by nature, handovers when in the external network force the mobile node to re-establish IPsec connectivity. Since this may be unacceptable in some scenarios, the IPsec tunnel can be made mobile by using Mobile IP underneath IPsec to provide for a static "outer" tunnel address (i.e. the Mobile IP home address obtained from the external home agent is used as the IPsec tunnel remote outer endpoint address).

NAT traversal is addressed by the Mobile IPv4 NAT specification [3] whenever applicable (i.e. when Mobile IP is the lowest layer protocol) and IPsec NAT traversal ([5], [6]) whenever applicable (i.e. when IPsec is the lowest layer protocol).

Note that this document does not specify how the mobile node detects it is in the external network and should try to establish an IPsec tunnel.

2.3 Scenarios

2.3.1 Mobile node in the intranet

2.3.1.1 Mobile node in the home subnet

No difference to standard Mobile IPv4; however, the mobile node MUST have some secure means of ensuring that it has indeed returned home. This document does not specify such a mechanism.

2.3.1.2 Mobile node uses a co-located intranet address

The mobile node acquires a care-of address e.g. using DHCP.

Site-to-site IPsec tunnels do not affect the registration (or routing) procedure other than that reverse tunnelling SHOULD be used to avoid problems with IPsec policy selectors. If the site-to-site IPsec tunnel is not a "bridging" tunnel, there is a different subnet at each end of the tunnel. In this case each IPsec tunnel endpoint MUST do a sort of ingress filtering as a part of IPsec policy

processing. Thus, reverse tunneling is required.

2.3.1.3 Mobile node uses an intranet foreign agent

No difference to standard Mobile IPv4.

2.3.1.4 Mobile node uses a trusted foreign agent in the external network

A trusted foreign agent, as described in [2], is located in the external network and would typically have a static IPsec tunnel to secure communication between the FA and the HA.

This scenario is essentially identical to using an intranet foreign agent from the home agent and mobile node perspectives. If there is a NAT device between the trusted foreign agent and the IPsec device, IPsec NAT traversal ([5], [6]) is required.

From the mobile node perspective, there MUST be a secure way to identify a trusted foreign agent. This document does not specify such a mechanism.

2.3.2 Mobile node in the external network, no external Mobile IP

The mobile node acquires an IPsec tunnel outer address using some unspecified means (manual configuration, DHCP, etc). The node then forms an IPsec tunnel using e.g. IKE.

The inner address of the tunnel is the one that is used to route traffic from the home network to the IPsec device. The mobile node has to obtain this address somehow, e.g. by manual configuration or by using the IPsec-DHCP mechanism [4]. If there is a NAT between the external home agent and the DHCP device, IPsec NAT traversal should be used ([5], [6]).

Once the IPsec tunnel has been formed, the mobile node uses the tunnel inner address as its co-located care-of address and proceeds with Mobile IPv4 registration normally.

Note that this scenario is a degenerated version of the site-to-site IPsec tunnel registration. Mobile IP reverse tunneling MUST be used for the same reason as with the site-to-site scenario.

2.3.3 Mobile node in the external network, using external Mobile IP

In these scenarios, Mobile IP is used as a mobility mechanism for transporting IPsec tunnel packets. There is an external home agent in the external network, and two logical mobile nodes (in the Mobile IP sense) in the mobile node host: one for the intranet home agent,

and another for the IPsec mobility home agent.

Since the external Mobile IP is only involved in transporting IPsec, there are no limitations on e.g. use of reverse tunnelling. Thus, packets sent by the mobile node can be, if desired, sent directly to the IPsec device without going through the external home agent (if ingress filtering is not in use).

2.3.3.1 Mobile node uses an external co-located care-of address

The mobile node obtains an external co-located care-of address e.g. using DHCP. The mobile node then uses this care-of address to register to the external Mobile IP home agent. If there is a NAT between the mobile node and the external home agent, Mobile IP NAT traversal [3] should be used.

Once the external mobility binding is set up, the mobile node can use the home address (from the external home agent address space) as an IPsec tunnel outer address. The inner address is still obtained e.g. by manual configuration or the IPsec-DHCP mechanism [4]. If there is a NAT between the external home agent and the DHCP device, IPsec NAT traversal should be used ([5], [6]).

Once the IPsec tunnel has been formed, the mobile node uses the tunnel inner address as its co-located care-of address and proceeds with Mobile IPv4 registration normally, this time registering to the intranet home agent.

Note that this scenario is a degenerated version of the site-to-site IPsec tunnel registration. Mobile IP reverse tunneling MUST be used for the same reason as with the site-to-site scenario.

2.3.3.2 mobile node uses an external foreign agent

The mobile node detects the foreign agent and registers to the external home agent using the foreign agent. If there is a NAT device between the external foreign agent and the external home agent, Mobile IP NAT traversal should be used [3].

Otherwise the scenario plays out as in Section 2.3.3.1.

2.4 Some issues

2.4.1 Use of reverse tunnelling

Since IPsec security associations are bound to the "inner" addresses, Mobile IP reverse tunneling MUST be used when registering through an IPsec device, using the tunnel "inner" address as a co-located care-

of address.

2.4.2 Detecting internal and external network

The mobile node needs a mechanism for detecting which scenario it is currently in, i.e. a mechanism to detect that it is in the outside network or in the intranet. A simple mechanism is to try registration without IPsec first, and if that consistently fails for a reasonable period of time, automatically try IPsec. If the mobile node makes an error, it is never fatal security-wise because the mobile node errs on the side of trying to set up the IPsec tunnel in vain.

2.4.3 Packet overhead

The solution does not optimize packet overhead. However, since only standard nodes are needed in the solution, some extra overhead may be acceptable.

2.4.4 Co-located care-of address registration through a foreign agent

When a mobile node registers using a co-located care-of address, a foreign agent can be used for the registration, although this case has not been explicitly covered in the scenarios.

2.4.5 Using an external foreign agent

If the mobile node must be able to communicate to the home network even when connected to an external foreign agent, use of Mobile IP underneath IPsec is no longer optional. Without the use of external Mobile IP, this access scenario will not work.

2.4.6 Mobile node network stack arhitecture considerations

The solution calls for changes in the composition of the mobile node network stack depending on whether the mobile node is outside or inside the home network. In particular, IPsec needs to be enabled or disabled (an effect that may also be achieved by configuring IPsec policy dynamically), and two instances of Mobile IP may be required, one underneath and one above IPsec.

Since the mobility bindings established through the IPsec tunnel are entirely transparent to the internal home agent, all Mobile IP features (e.g. simultaneous bindings) can be used in the solution. In addition, the mobile node is free to do split tunnelling, although it places more requirements on the architecture of the mobile node network stack.

2.4.7 AAA considerations

TBD

3. Acknowledgements

The authors would like to thank colleagues at Netseal, especially Ilkka Pietikainen and Timo Aalto, and people on the the MIP/VPN coexistence mailing list, especially Farid Adrangi and Alan O'Neill, for feedback on the approach.

References

[1] Perkins, C., "IP Mobility Support for IPv4", RFC 3220, January 2002.

[2] Adrangi, F., Iyer, P., Leung, K., Kulkarni, M., Patel, A., Zhang, Q. and J. Lau, "Problem Statement for Mobile IPv4 Traversal Across VPN Gateway (draft-ietf-mobileip-vpn-problem-statement-00)", March 2002.

[3] Levkowetz, H. and S. Vaarala, "Mobile IP NAT/NAPT Traversal using UDP Tunnelling (draft-ietf-mobileip-nat-traversal-04)", May 2002.

[4] Patel, B., Aboba, B., Kelly, S. and V. Gupta, "DHCPv4 Configuration of IPsec Tunnel Mode (draft-ietf-ipsec-dhcp-13)", June 2001.

[5] Kivinen, T., Huttunen, A., Swander, B. and V. Volpe, "Negotiation of NAT-Traversal in the IKE (draft-ietf-ipsec-nat-t-ike-03)", June 2002.

[6] Huttunen, A., Swander, B., Stenberg, M., Volpe, V. and L. DiBurro, "UDP Encapsulation of IPsec Packets (draft-ietf-ipsec-udp-encaps-03)", June 2002.

Authors' Addresses

Antti Nuopponen
Netseal
Niittykatu 6
P.O.Box 38
Espoo FIN-02201
Finland

EMail: antti.nuopponen@netseal.com

Sami Vaarala
Netseal
Niittykatu 6
P.O.Box 38
Espoo FIN-02201
Finland

EMail: sami.vaarala@iki.fi

Full Copyright Statement

Acknowledgement

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