Internet Engineering Task Force
INTERNET DRAFT
Category: Informational

Farid Adrangi
Prakash Iyer
Intel Corp.

<draft-adrangi-mobileip-nat-vpn-problem-stat-req-00>
Date: January 2002

Problem Statement and Requirements for Mobile IPv4 Traversal Across VPN or 'NAT and VPN' Gateways

Status of this Memo

Abstract

This draft describes the problem statement and specifies the solution requirements for MIPv4 traversal across VPN or 'NAT and VPN' gateways. The 'NAT and VPN' case refers to a network topology in which the MIPv4 traffic has to traverse one or more NAT gateway(s) followed by a VPN gateway in the path to its final destination. Requirements and problems associated with MIPv4 traversal through NAT gateways NOT involving VPNs is

outside the scope of this draft.

Table of Contents

---

1. Introduction.....2
2. Terminology.....3
3. Acronyms.....3
4.0. Roaming Scenarios.....4
4.1. Roaming Inside the Home Network.....5
4.2. Roaming Outside the Home Network.....5
4.2.1. Roaming Outside the Home Network in a Routable Address Space (where, FA-assisted routing is not used).....6
4.2.2 Roaming Outside the Home Network in Routable Address Space (where, FA-assisted routing is used).....6
4.2.3 Roaming Outside the Home Network in a non-Routable Address Space.....7
5. Problem Statement.....8
5.1. MIPv4 Incompatibilities with VPN Gateways.....8
5.2. MIPv4 Incompatibilities with NAT Gateways.....9
6. The Requirements.....9
6.1. Implications of Intervening NAT Gateways.....9
6.2. Implications of Cascaded NAT.....10
6.3. MIPv4 Protocol.....10
6.5. Functional Entities.....10
6.6. Multi-vendor Interoperability.....10
6.7. Fast MIPv4 Handoffs.....10
6.8. Preservation of Existing VPN Infrastructure.....11
6.9. Preserve Existing DMZ Traversal Policies.....11
6.10 Support For Route Optimization.....11
6.11 MIPv4 Registration SA Management.....11
6.12 Security Implications.....11
7. References.....11

1. Introduction

Multi-subnetted IEEE 802.11 WLAN networks are being widely deployed in Enterprise Intranets - in many cases requiring a VPN tunnel to connect back and access Intranet resources, and public areas such as airports, coffee shops, convention centers and shopping malls. Many of these WLAN networks also employ NAT

to translate between non-routable and routable IPv4 care-of (point of attachment) addresses. WWAN networks such as those based on GPRS and eventually EDGE and UMTS are also starting to see deployment. These deployments are paving the way for applications and usage scenarios requiring TCP/IP session persistence and constant reachability while connecting back to a secured (VPN protected), target 'home' network. This in turn drives the need for a mobile VPN solution that is multi-vendor interoperable, providing seamless access with persistent VPN sessions and through NAT gateways when needed. This draft identifies example usage scenarios, defines a problem statement based on the scenarios and specifies requirements that MUST be met to ensure broad deployment of multi-vendor interoperable solutions.

The important sections of this draft are organized as follows:

Section 4: Describe roaming scenarios to motivate the problem statement

Section 5: Describes a problem statement for MIPv4 traversal across VPN and NAT gateways.

Section 6: Specifies the requirements for a solution to support multi-vendor seamless IPv4 mobility across VPN or the 'NAT VPN' gateways.

2. Terminology

Traditional NAT:
Network Address Translation. "Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network." ' [RFC2663]. Traditional NAT' are of two types: Basic NAT and NAPT.

Basic NAT:
"With Basic NAT, a block of external addresses are set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, the source IP address and

related fields such as IP, TCP, UDP and ICMP header checksums are translated. For inbound packets, the destination IP address and the checksums as listed above are translated." û [RFC2663]

NAPT:
Network Address Port Translation. "NAPT extends the notion of translation one step further by also translating transport identifier (e.g., TCP and UDP port numbers, ICMP query identifiers). This allows the transport identifiers of a number of private hosts to be multiplexed into the transport identifiers of a single external address. NAPT allows a set of hosts to share a single external address. Note that NAPT can be combined with Basic NAT so that a pool of external addresses are used in conjunction with port translation." û [RFC2663]

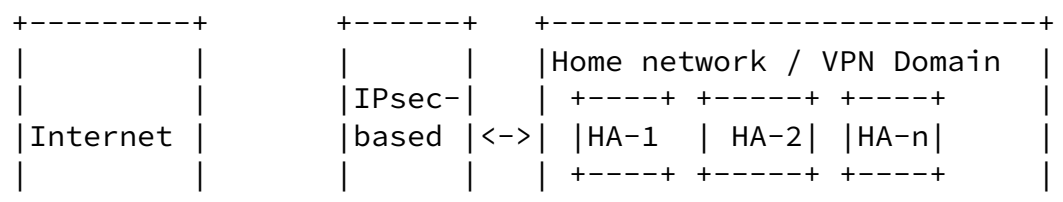
3. Acronyms

ACL: Access Control List
GRE: Generic Routing Encapsulation
MIPv4: Mobile IP for IPv4
MIPv6: Mobile IP for IPv6
VPN: Virtual Private Network

MN-Perm: Permanent home address of the MN
MN-COA: Co-located care-of address of the MN
WLAN: IEEE 802.11 Wireless Local Area Network

4.0. Roaming Scenarios

This section describes roaming scenarios, wherein MIPv4 traffic has to traverse VPN or the 'NAT and VPN' gateways. The scenarios are constructed based on a multi-subnetted MIPv4 enabled Intranet (hereafter, referred by Home Network or VPN domain) protected by an IPsec-based VPN gateway as depicted in Figure 4.0a.



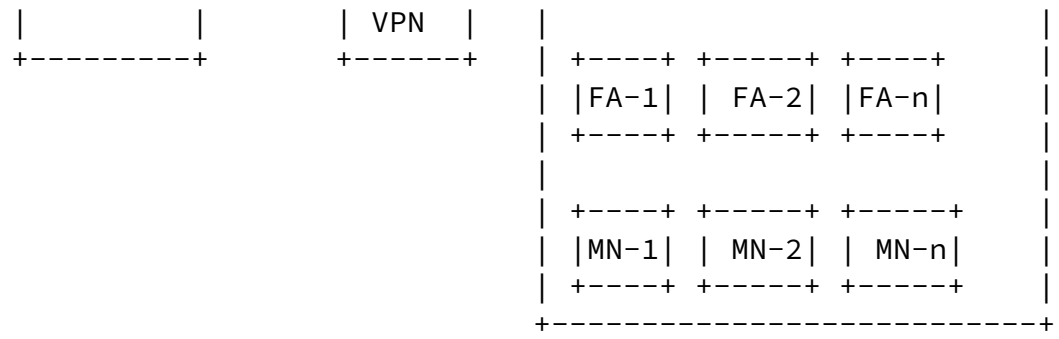


Figure 4.0a Home Network protected by a VPN Gateway

The home network, depicted in Figure 4.0a, may include both wired (IEEE 802.3) and IEEE 802.11 wireless LAN deployments. However, it is also possible to see IEEE 802.11 deployments outside the home network due to perceived lack of 802.1x security, as depicted in Figure 4.0b.

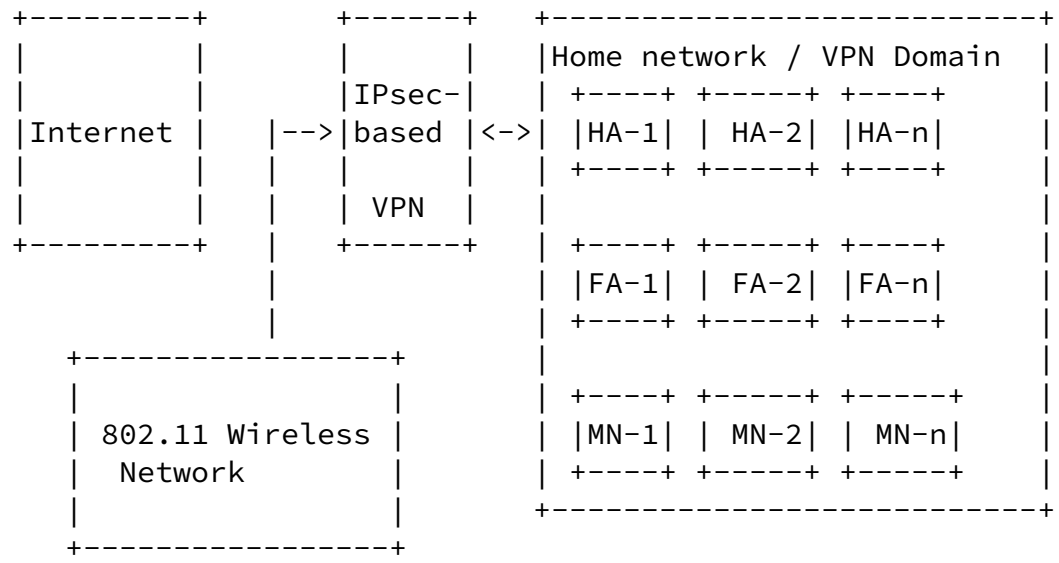


Figure 4.0b' IEEE 802.11 Wireless deployment outside the home network

To help describe scenarios in the following sections, we have used the aid of an imaginary nomadic user, called Dr. Joe. Dr. Joe is a chief surgeon in a hospital, and always on the move. He leverages his wireless MIPv4 enabled hand-held device

to access his patient' records, communicate with his colleagues and staff, and stay reachable in case of any emergencies. For clarity, we assume that Dr. Joe' hospital employs a network similar to the one showed in Figure 4.0a (MIPv4 enabled network protected by a VPN, and includes both wired and IEEE 802.11 wireless deployments).

4.1. Roaming Inside the Home Network

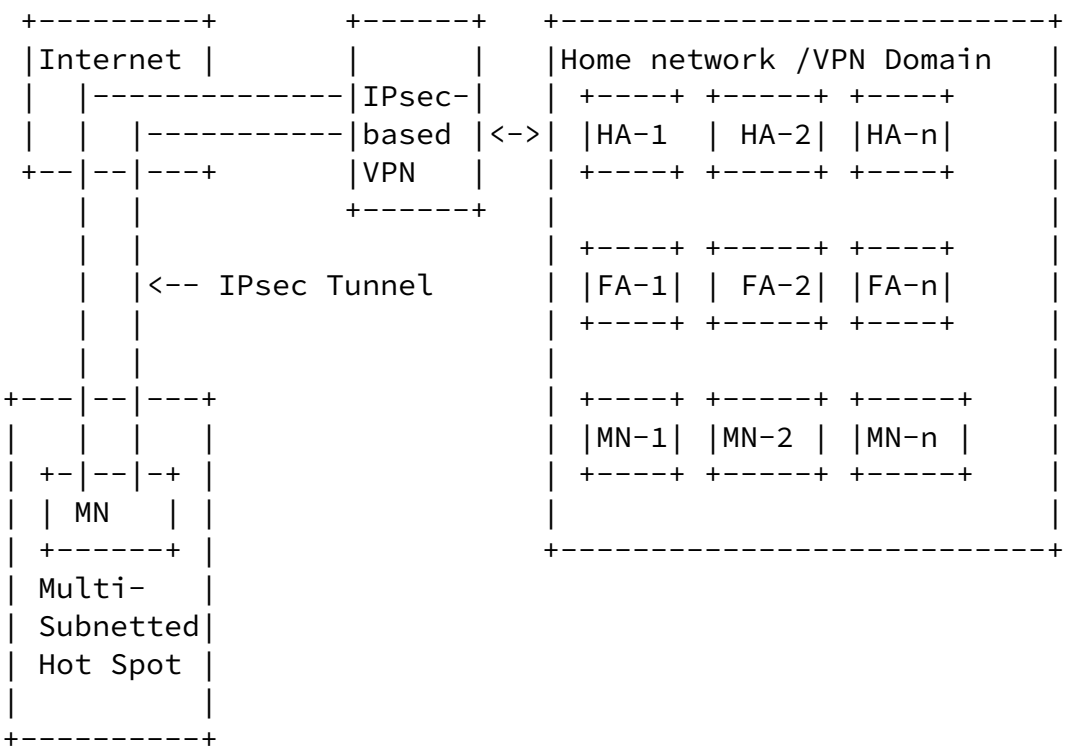
Dr. Joe' needs for constant reachablity and maintaining his current transport connections as he roams from one network link to another are met by standard MIPv4 deployment inside the home network. Please note that NATÆed networks might be seen inside the home network, however, draft-mobileip-nat-traversal-00.txt solves the problem, as the mobile node's home agent will most likely be directly reachable by the mobile node.

4.2. Roaming Outside the Home Network

Dr. Joe frequently visits other clinics and hospitals, in which a multi-subnetted IEEE 802.11 hot spot network is utilized to provide Internet access for visitors. Dr. Joe leverages the hot spot network to connect to his home network, and he would also like to maintain his transport connections to the home network as he roams from one network link to another in the hot spot network.

This implies that the MIPv4 traffic destined to the home network MUST run inside an IPsec tunnel (i.e, MIP/IP/ESP/IP) established between the mobile node and the home networkÆs VPN gateway. Moreover, the IPsecÆed MIPv4 traffic may also have to traverse a NAT gateway or a foreign agent in the path to the VPN gateway. The following sub-sections illustrate these possibilities.

4.2.1. Roaming Outside the Home Network in a Routable Address Space (where, FA-assisted routing is not used)



4.2.2 Roaming Outside the Home Network in Routable Address Space (where, FA-assisted routing is used)

There is a notion of trusted FA, where there is a SA established between the FA and home VPN gateway. In this case, IPsec tunnel end-points are the FA and home VPN gateway. Furthermore, It is also possible for the MN in a trusted FA region to have end-to-end security with its home VPN gateway. This implies that there will be two pairs of IPsec tunnels, one between the FA and home VPN gateway, and the other between the MN and its home VPN gateway. Figure 4.3.2a shows the MN in a trusted FA region, where there is only an IPsec tunnel between the FA and home VPN gateway.

In a non-trusted FA region, where there is no SA established between the FA and home gateway, there will always be a single IPsec tunnel established between the MN and its home VPN gateway, as depicted in Figure 4.3.2b.

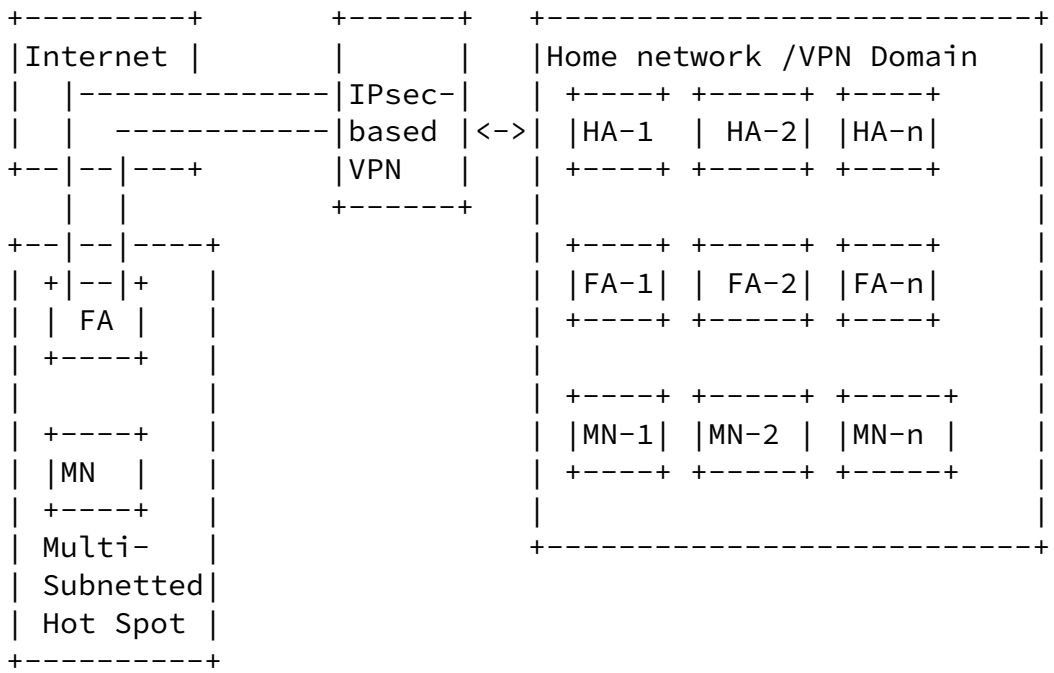
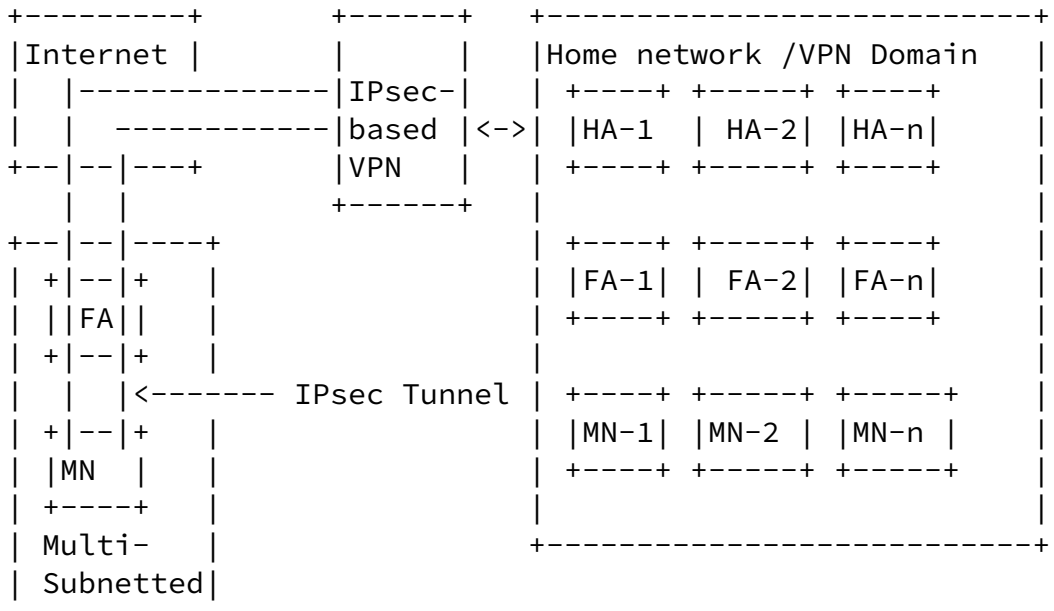


Figure 4.3.2a - the MN in trusted FA region



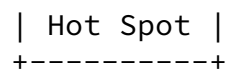
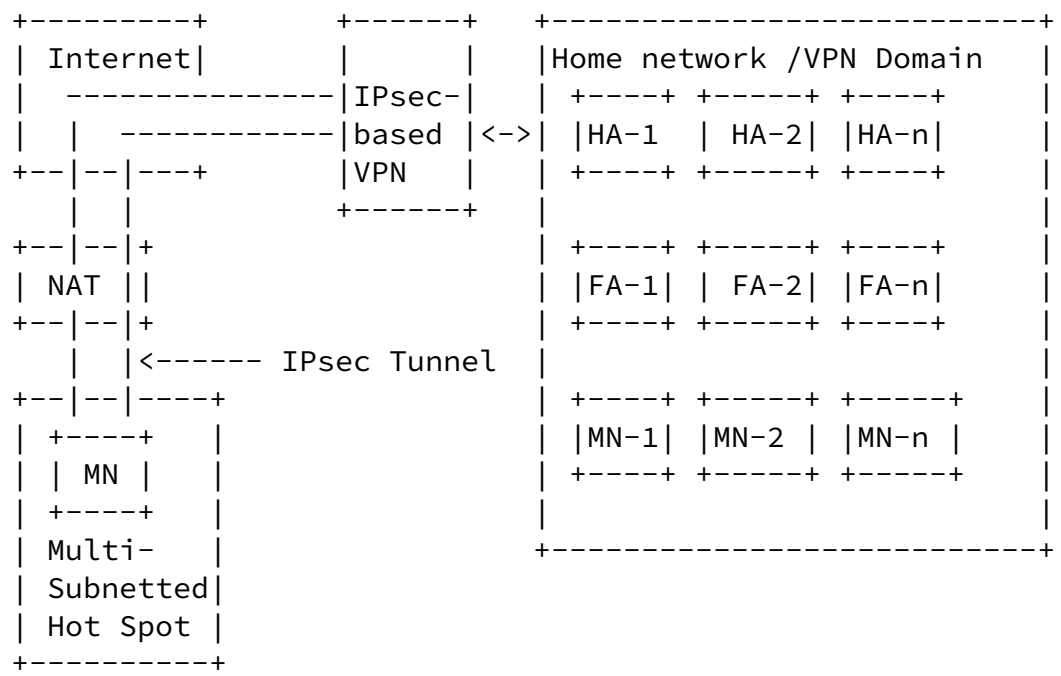


Figure 4.3.2b - the MN in non-trusted FA region

4.2.3 Roaming Outside the Home Network in a non-Routable Address Space

Note that the MN's home agent is not directly reachable in this case. Therefore, draft-mobileip-nat-traversal-00.txt cannot be directly applied. Furthermore, cascaded NAT gateway

deployment is also a possibility, but not shown in the diagram.



5. Problem Statement

This section describes MIPv4 incompatibilities with IPsec-based VPN and NAT gateways, in the context of the roaming scenarios outlined in section 4.

5.1. MIPv4 Incompatibilities with VPN Gateways

There are two problems associated with MIPv4 and VPN incompatibilities.

Problem 1: The MN could roam into a foreign subnet with a FA. If the MN were to associate a VPN tunnel with its CoA, the FA (which is likely in a different administrative domain) cannot parse the IPsec tunnel SA and will not be able to setup SAs with the MN's VPN gateway and will consequently be not able to relay MIPv4 packets between the MN and the VPN gateway.
`

Problem 2: The MN could roam into a foreign subnet without a FA and obtain a CoA at its point of attachment (via [DHCP] or some other means). In an end-to-end security model, an IPsec tunnel that terminates at the VPN gateway MUST protect the IP traffic originating at the MN. If the IPsec tunnel is associated with the CoA, the tunnel SA MUST be refreshed after each IP subnet handoff which could have some performance implications on real-time applications.

It is important to note that only IPsec tunnel mode is applicable here, as the mobile node connecting to the home network MUST establish an IPsec tunnel SA to the VPN gateway.

5.2. MIPv4 Incompatibilities with NAT Gateways

There are also two problems associated with MIPv4 and NAT incompatibilities:

Problem 1: When an MN roams from its 'home' network (which may or may not be in a routable IP address space) protected by a VPN to a foreign network behind a NAT gateway, it acquires a non-routable care-of address (most likely through [DHCP]). The acquired non-routable care-of address is passed to the HA through a registration request. This causes the MN to lose its connectivity to its home network, since the HA will not be able to forward the MN's packets to the non-routable care-of address.

Problem 2: Even if we solve the first problem, an intervening NAT gateway in a foreign network will not always be able to demultiplex inbound IP-in-IP reverse tunneled MIPv4 data packets. Because, NAPT gateways will simply not be able to route the inbound IP-in-IP packets, as they rely on IP address and transport identifier to route the packets from routable to non-routable address space or vice a versa. And, in the case of Basic NAT, consider two MNs that are registered with the same Home Agent (HA). The inbound packets destined to the two MNs from the HA will have the same source and destination IP addresses ' making it difficult for the NAT to route the packets inside.

The implications on Minimal IP [RFC2004] and GRE encapsulation [RFC1701] modes of MIPv4 are similar to IP-in-IP tunneling.

Draft [MIP-NAT] describes a solution to the NAT traversal problem when VPNs are not involved. In this draft, we only discuss NAT traversal requirements where the HA is behind a VPN gateway and hence not directly reachable by the MN.

6. The Requirements

This section describes the requirements that are intended to establish a framework where in a solution can be developed to support MIPv4 traversal across VPN or 'NAT and VPN' gateways.

6.1. Implications of Intervening NAT Gateways

- The solution MUST work with both Basic NAT and NAPT.

- The solution MUST not require any configuration or software changes to exiting NAT gateways.

The reason for the above constraints is to not limit the solution to network topologies that employ certain types of NAT gateways and to enable deployment of MIPv4 in networks that have currently deployed non-modifiable NAT gateways.

6.2. Implications of Cascaded NAT

Cascaded NAT deployment is seen in some network topologies (case in point, a residential NAT gateway connected to a NATÆed ISP network). Therefore, the solution MUST support cascaded NAT.

6.3. MIPv4 Protocol

- The solution MUST be compliant with MIPv4 protocol [RFC 3220].
- The solution MAY introduce new extensions to MIPv4 protocol per guidelines specified in the MIPv4 RFCs. However, it is highly desirable to avoid any changes to MIPv4 mobility agents such as the FA and HA in order to overcome barriers to deployment.

6.5. Functional Entities

The solution MAY introduce a MIPv4 compliant functional entity that helps MIPv4 traversal across VPN or the ôNAT and VPNö gateways. However, scalability, manageability and availability implications introduced by that functional entity MUST be well understood. The functional entity MAY be implemented as a standalone entity or combined with another device such as a VPN gateway.

6.6. Multi-vendor Interoperability

Multi-vendor interoperability is a key requirement. In most Enterprises, MIPv4 mobility agents are likely to be deployed in existing routers from vendor X while VPN client/server solutions may come from vendor Y and mobility clients (MN) may come from yet another vendor. Medium and large Enterprises that typically purchase and deploy best-of-breed multi-vendor solutions for IP routing, VPNs, firewalls etc. are unlikely to revamp their infrastructure in favor of single-vendor end-to-end integrated solutions, preferring instead to reuse as much of their deployed infrastructure as possible. The solution proposed MUST enable such scenarios to be easily accommodated.

6.7. Fast MIPv4 Handoffs

It is imperative to keep the key management overhead down to a minimum, in order to support fast handoffs across IP subnets. Hence, the solution MUST propose a mechanism whereby the IPsec tunnel SA can be bound to the invariant home IP address of the MN and applicable to static and dynamic home address assignment.

6.8. Preservation of Existing VPN Infrastructure

This implies the following:

- The solution MUST preserve the investment in existing VPN gateways
- The solution MAY require software upgrades to VPN gateways to explicitly support MIPv4 users

- The solution MUST preserves VPN security requirements that are not inferior to what is already provided to existing "nomadic computing" remote access users, i.e. for confidentiality, primary and secondary authentication, message integrity, protection against replay attacks and related security services.

6.9. Preserve Existing DMZ Traversal Policies

The solution MUST be compatible with existing DMZ policies with respect to ACLs.

6.10 Support For Route Optimization

MIPv4 route optimization is not widely supported, as it requires changes to both MN's home agent and the correspondent node. Hence, The solution MAY or MAY NOT support MIPv4 Route Optimization [ROUTE-OPT].

6.11 MIPv4 Registration SA Management

Mechanisms to manage MIPv4 Registration SAs are outside the scope of this draft.

6.12 Security Implications

The solution MUST NOT introduce any new vulnerabilities to the MIPv4 protocol as specified in related RFCs.

7. References

[RFC3220] RFC 3220 ' IP mobility support for IPv4
[RFC3024] RFC 3024 ' Reverse tunneling for mobile IP
[RFC2004] RFC 2004 ' Minimal encapsulation within IP

[RFC1701] RFC 1701 ' Generic Routing encapsulation

[RFC2119] RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels
[RFC1918] RFC 1918 ' Address Allocation for Private Internets
[RFC2663] RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations
[DHCP] RFC 2131 ' Dynamic Host Configuration Protocol
[MIPv4-SEC-GUIDE] draft-bpatil-mobileip-sec-guide-01.txt - Requirements / Implementation Guidelines for Mobile IP using IP Security
[[LOCAL-LINK] ' Dynamic Configuration of Iv4 Link-Local Addresses, <draft-ietf-zeroconf-ipv4-linklocal-03>
[ROUTE-OPT] ' Route Optimization in Mobile IP, <draft-ietf-mobileip-optim-10.txt>
[MIP-NAT]' Mobile IP NAT/NAPT Traversal using UDP Tunneling, <draft-mobileip-nat-traversal.00.txt>

Authors:

Farid Adrangi
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR
USA

Phone: 503-712-1791
Email: farid.adrangi@intel.com

Prakash Iyer
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR
USA

Phone: 503-264-1815
Email: prakash.iyer@intel.com