Internet Engineering Task Force
INTERNET DRAFT
Category: Informational

Farid Adrangi
Prakash Iyer
Intel Corp.

Kent Leung
Milind Kulkarni
Alpesh Patel
Cisco Systems

Qiang Zhang
Liqwidnet Inc.

Joe Lau
Hewlett Packard Corp.

<draft-ietf-mobileip-vpn-problem-statement-00>
Date: March 2002

Problem Statement for Mobile IPv4 Traversal Across VPN Gateways

Status of this Memo

Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

Mobile IP [1] agents are being deployed in enterprise networks, to enable mobile users with network mobility across wired and wireless LANs while roaming inside the enterprise firewall. With the growing deployment of multi-subnetted IEEE 802.11 networks (referred as hot spots) in public places such as hotels, airports, and convention centers, and wireless WAN data networks such as GPRS, the need for enabling mobile users to maintain their transport connections and constant reachability while connecting back to their target ôhomeö networks protected by VPNs is increasing. This draft identifies example usage scenarios for enterprise users roaming outside the firewall, and defines a problem statement based on the scenarios.

Table of Contents

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. Wireless WAN 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 ôhomeö network. This in turn drives the need for a mobile VPN solution that is multi-vendor interoperable, providing seamless access with persistent VPN sessions. This draft identifies example usage scenarios, and defines a problem statement based on the scenarios.

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 gateways.

2. Terminology

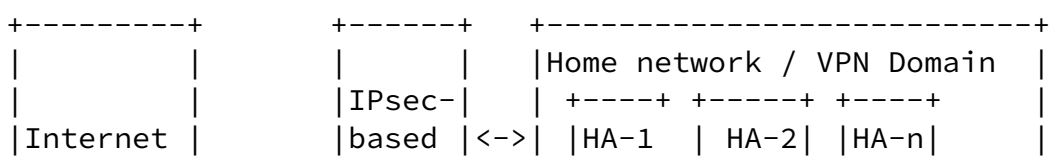
3. Acronyms

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

MN-HoA: Permanent home address of the MN
MN-CoA: Co-located care-of address of the MN
VPN_E_Addr: VPN Gateway External IP Address
WLAN: IEEE 802.11 (a/b/g) Wireless Local Area Network

4.0. Roaming Scenarios

This section describes roaming scenarios, wherein a mobile user roaming outside the firewall needs to connect to his/her ôtargetö home network protected by a VPN. 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.



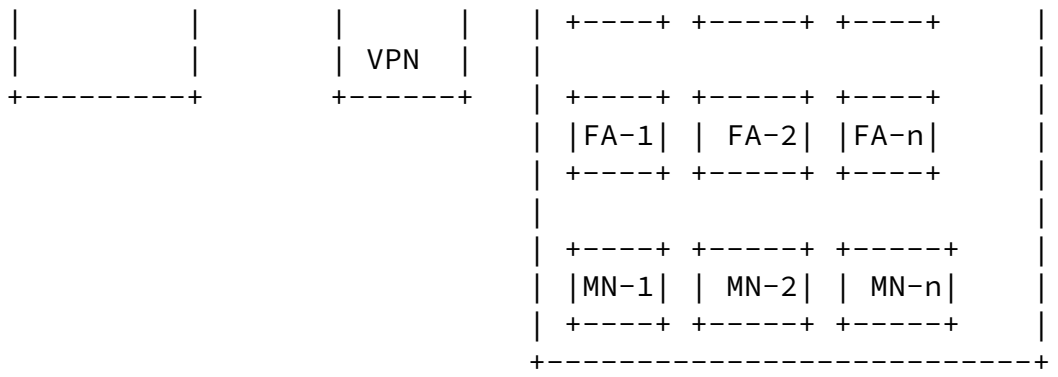


Figure 4.0a û Home Network protected by a VPN Gateway

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 the perceived lack of 802.1x security, as depicted in Figure 4.0b.

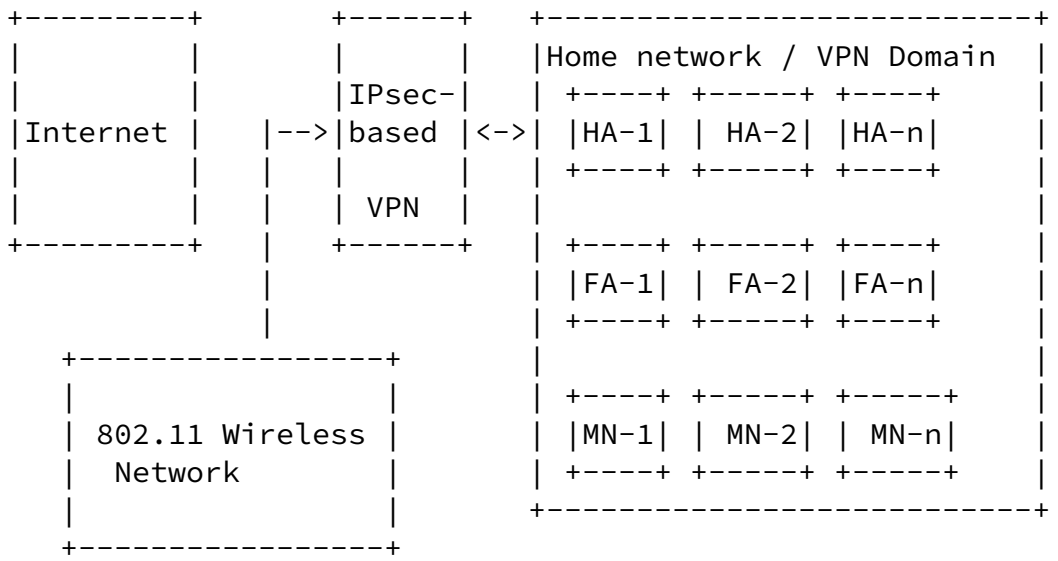


Figure 4.0b û IEEE 802.11 Wireless deployment outside the home network

It is important to note that MIPv4 mobility agents inside the home network 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. This is very typical as medium and large Enterprises purchase and deploy best-of-breed multi-vendor solutions for IP routing, VPNs, firewalls etc.

To help describe scenarios in the following sections, we have used the aid of an imaginary mobile 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 patientÆs records, communicate with his colleagues and staff, and stay reachable in case of any emergencies. For clarity, we assume that Dr. JoeÆs 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. Accessing Services Inside the Home Network

Dr. JoeÆs needs for constant reachablity and maintaining his current transport connections as he roams from one network link to another are met by standard MIPv4 [1] deployment inside the home network.

4.2. Accessing Services From 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 visited network.

Dr. Joe needs to establish an IPsec tunnel to the VPN gateway first so that he can register with the home agent while roaming outside the home network. This implies that the MIPv4 traffic destined to the home network has to run inside an IPsec tunnel.

The different registration modes of the MN are described in

sections below.

5.0. Operational Configurations

5.1. MN registers with its HA using co-located mode

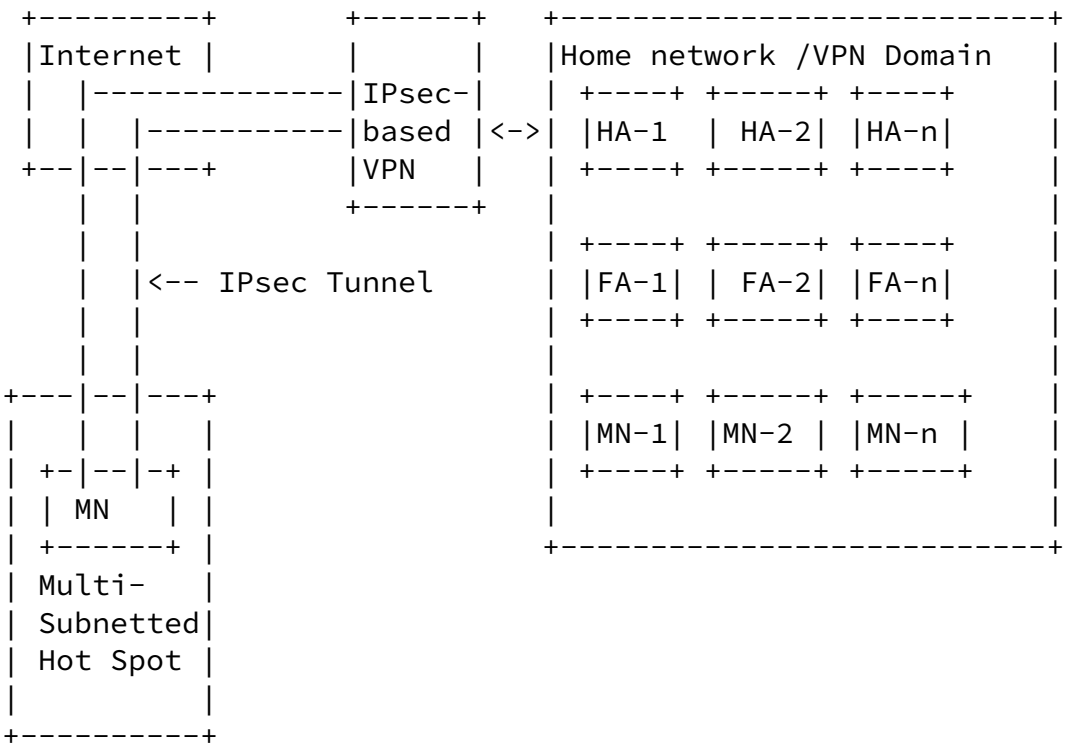


Figure 5.1.

5.2. MN registers with its HA via a FA (non co-located mode)

There are 2 cases to consider.
Case 1:
The FA is trusted, i.e. an SA has been established a priori between the FA and the home VPN gateway. In this case, the 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 concurrent IPsec tunnels, one between the FA and home VPN gateway, and the other between the MN and its home VPN gateway. Figure 5.2a shows the MN in a trusted FA region, where there is only an IPsec tunnel between the FA and the home VPN gateway.

Case2:
In a non-trusted FA region, i.e. where there is no SA between the FA and the home VPN gateway, there will always be a single IPsec tunnel established between the MN and its home VPN gateway, as depicted in Figure 5.2b.

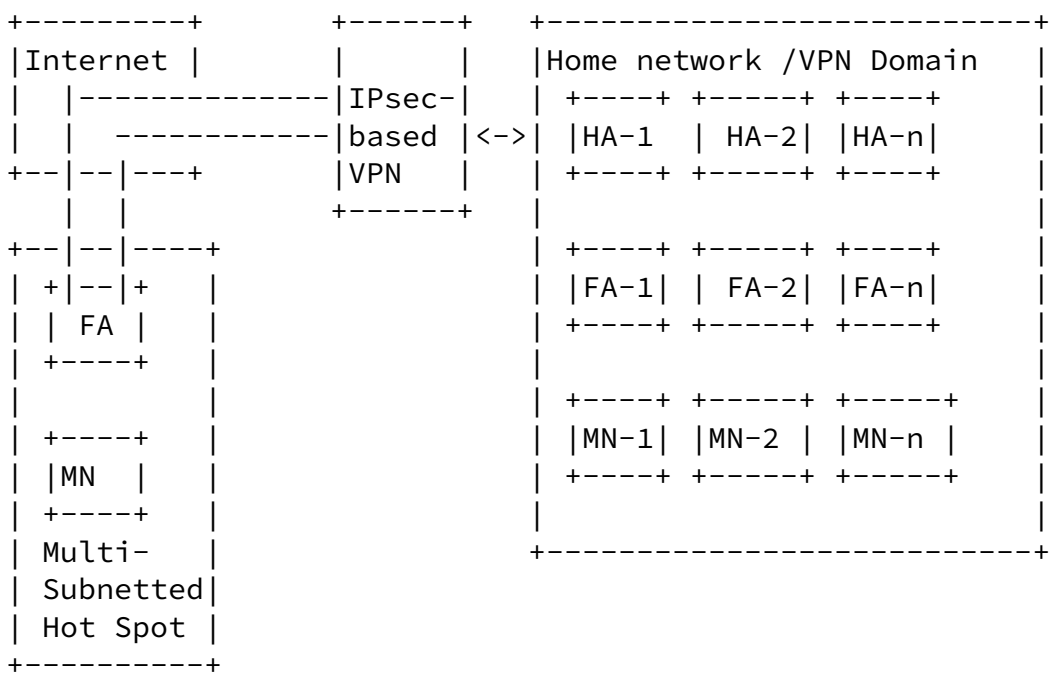


Figure 5.2a - the MN in trusted FA region

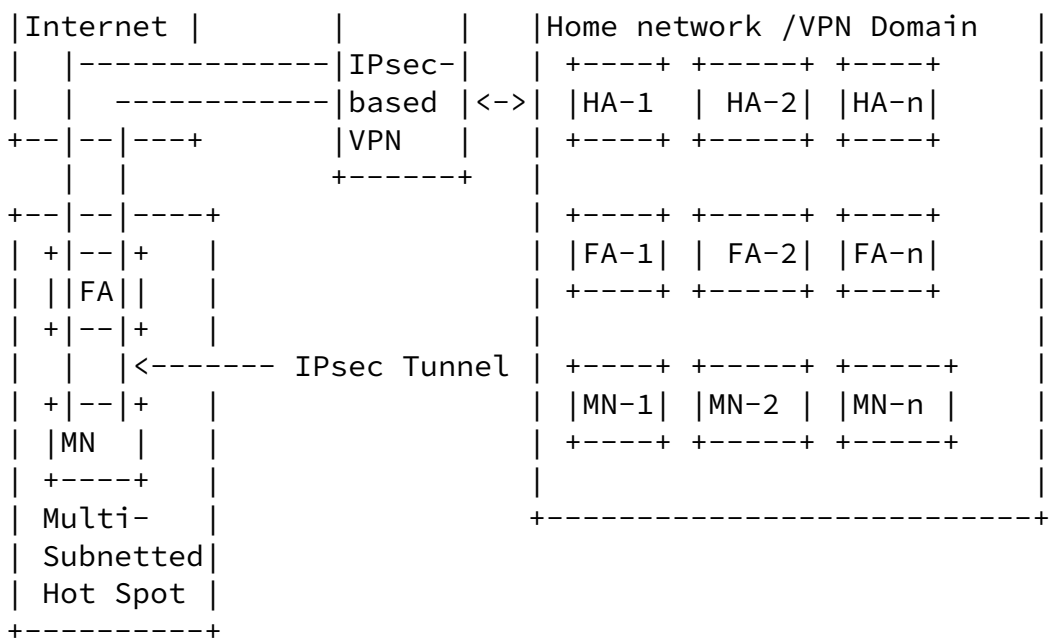


Figure 5.2b - the MN in non-trusted FA region

6. Problem Statement

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

6.1. MIPv4 Incompatibilities with VPN Gateways

The MN roaming outside the home network has to establish an IPsec tunnel to its home VPN gateway first, in order to be able to register with its home agent. Figure 6.1a and 6.1b show the tunnel end-points in non co-located and co-located modes respectively.

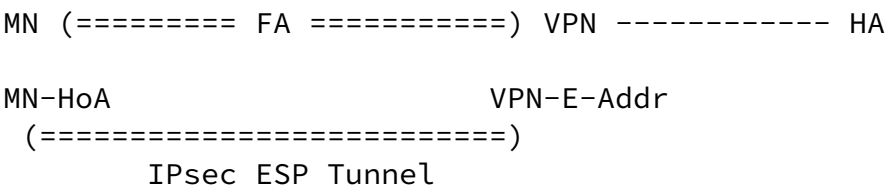


Figure 6.1a û Shows IPsec Tunnel end-points, MN Home Address and VPN External IP Address, in non co-located mode

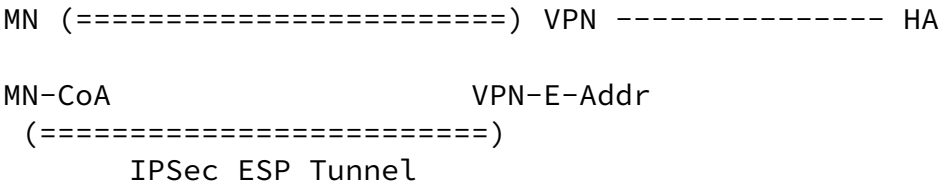
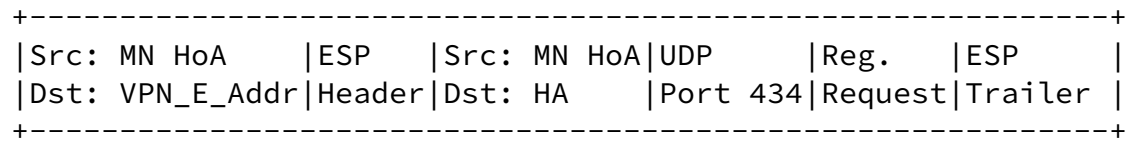


Figure 6.1b û Shows IPsec tunnel endpoints, MN-CoA and the VPN External IP address, in co-located mode

This implies that the MIPv4 traffic has to run inside IPsec tunnel, and will not be in the clear. This leads to the following problems:

Problem 1: In non co-located mode, this implies that the FA (which is likely in a different administrative domain) cannot decrypt MIPv4 packets between the MN and the VPN gateway, and will consequently be not able to relay the MIPv4 packets. For example, the following shows the MNÆs registration packet arrived at FA, which cannot be decrypted by the FA.



Problem 2: In co-located mode, the MN obtains a CoA at its point of attachment (via DHCP[7] 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 first.

7. MIPv6 Considerations

MIPv6 does not have a FA component, hence the MN will always run in co-located mode. This implies that only problem #2 specified in the problem statement (section 6.1) is applicable to MIPv6.

8. Revisions History

1) Initial Version March 2002

2) Second Version April 2002
   + Modified the draft based on Phil Roberts comments.

1. NAT section was removed
2. Solution requirements section was removed
3. Tunnel end-point are clearly identified

+ Made minor organizational changes as Phil Roberts requests
1. Make Dr. Joe section more generic
2. Split 4.0 section

9. References

[1] RFC 3220 û IP mobility support for IPv4
[2] RFC 3024 û Reverse tunneling for mobile IP
[3] RFC 2004 û Minimal encapsulation within IP
[4] RFC 1701 û Generic Routing encapsulation
[5] RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels
[6] RFC 1918 û Address Allocation for Private Internets
[7] RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations
[8] RFC 2131 û Dynamic Host Configuration Protocol

[9] draft-bpatil-mobileip-sec-guide-01.txt - Requirements / Implementation Guidelines for Mobile IP using IP Security
[10] Dynamic Configuration of IPv4 Link-Local Addresses, <draft-ietf-zeroconf-ipv4-linklocal-03>

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

Kent Leung Email: kleung@cisco.com Phone: 408-526-5030
Milind Kulkarni Email: mkulkarn@cisco.com Phone: 408-527-8382
Alpesh Patel Email: alpesh@cisco.com Phone: 408-853-9580

Cisco Systems
170 W. Tasman Drive,
San Jose, CA 95134

Qiang Zhang Email: qzhang@liqwident.com
Phone: 703 8641327
Liqwidnet Inc.

Joe Lau Email: jlau@cup.hp.com Phone: 408 447-2159
Hewlett-Packard Company
19420 Homestead Road, MS 4301
Cupertino, CA 95014