

# Building ALL-IP Based Virtual Private Networks in Mobile Environment

Reinhard Ruppelt, Andrei Pelinescu, Cristian Constantin, John Floroiu, Dorgham Sisalem, Berthold Butscher

FOKUS, Berlin, Germany

{ruppelt, pelinescu, constantin, floroiu, sisalem, butscher}@fokus.gmd.de

## *Abstract*

*Security mechanisms such as firewalls commonly deployed throughout the Internet present serious obstacles to basic usage of Mobile IP. In this paper we describe how IP security mechanisms can be integrated with Mobile IP to create a mobile VPN. In this context, this work describes a prototype implementation of an integrated environment for secure, inter-domain, mobile communications for an existing corporate-like intranet of a public authority. In this paper the particular architecture of the deployment scenario and the implementation of the solution are described.*

**Keywords:** *Secure Mobile Networking, Mobile IP, IPsec, Firewall Traversal, Remote Access*

## 1. Introduction

Mobile IP [4] is a network layer protocol that aims at enabling mobile nodes to be addressable under the same IP address despite changes in their point of attachment to the Internet. Mobile IP therefore supports global mobility of Internet hosts and is one of the main candidates for IP mobility support in future All-IP networks. Further, the interworking between Mobile IP, IPsec<sup>1</sup> and authentication, authorization and accounting (AAA) infrastructures enables the creation of a framework for secure communication, dynamic service provisioning and seamless handover for mobile nodes.

In this paper we present a case study involving the development, deployment and testing of a mobile virtual private network (VPN) solution based on Mobile IP and IPsec protocols implemented in an existing large geographical distributed governmental intranet. Main goal of this case study was to evaluate the operational deployment of the technology in a governmental intranet with strong security requirements. In this context we

describe the different required components and their interaction among each other.

## 2. Supporting Mobile VPNs Using Mobile IP

The basic scenario to be realized in the work presented here, was to allow a governmental employee traveling from one location to another one belonging to the same authority to be reachable under a constant IP address and to access his home environment including files and servers in a transparent and secure manner. The scenario represents a firewall traversal solution aimed at protecting the home environments from intrusion.

In this pilot realization an infrastructure was established which enabled the trial participants to access their home working environments regardless of their current point of attachment to the organizational intranet. Additionally, the solution was extended by an external access enabled by a dial-in remote access server. Strong requirements on the availability, privacy and integrity of the communication had to be ensured by the proposed architecture. The field test was carried out to determine the possibilities and boundaries of the technology with respect to the requirements of the users in terms of security and support of mobility.

The main aspects of this pilot attempt were

- the assessment of the effort necessary for a governmental wide deployment, and
- the practical testing of Mobile IP based mobility support in a governmental Intranet.

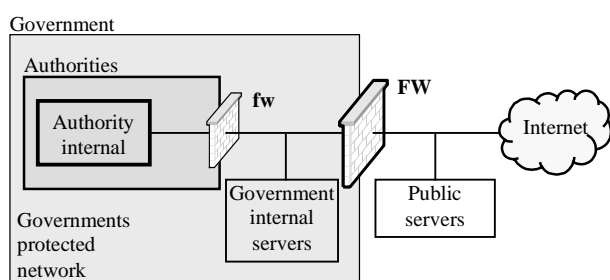
The implementation of the desired functionality was based here on the communication paradigm given by Mobile IP: to enable a mobile node (MN) to move within the Internet completely transparent, i. e., a MN is always subject to the same communication conditions regardless of its current point of attachment to the intranet.

The scenario for a mobility enhanced intranet environment is built by mobility- and security specific components (mobility servers and –clients, security gateways) placed in the corresponding subnetworks and at a central intranet firewall (FW). A subset of 3 authorities participates in the trial.

## 2.1. Infrastructure Requirements

The original structure of the government network was as follows: All authorities are connected by a central firewall controlling the entire traffic between the different authorities. All authorities are completely autonomous. Access is granted to internal users only. Each department’s interior network is insulated from the Internet by a perimeter network (DMZ). Each department is protected by a department specific firewall system (interior router (fw)). Behind this system, government internal servers provide several services for all users of an authority. A central firewall (exterior router (FW)) controls the entire traffic between the different authorities and protects the governmental intranet against the public internet. Connected to the firewall are also all public servers. All communication between the authorities is encrypted at the application level by means of dedicated hardware.

Originally there was no mobility support. IP addresses are statically allocated. No dynamic address assignment is supported. Throughout the whole governmental intranet private IP addresses [1] are used to hide the topology of the internal network. These addresses are not advertised to the general Internet and not directly routable from the outside Internet. The basic logical structure of the present IT infrastructure is as follows:



**Figure 1: Screened-Subnet Firewall Architecture**

The main requirements of the mobility extension of the governmental intranet were as follows:

1. Authorized employees of the authority must not suffer any loss of connectivity to resources in their home network independent of the authority they are connected to.

2. The governmental intranet must not be exposed to any new security threats caused by the deployment of the mobility feature.
3. A dial-up access should support external connections on the basis of the Point-to-Point Protocol (PPP [1]) and strong CHAP [3] authentication.

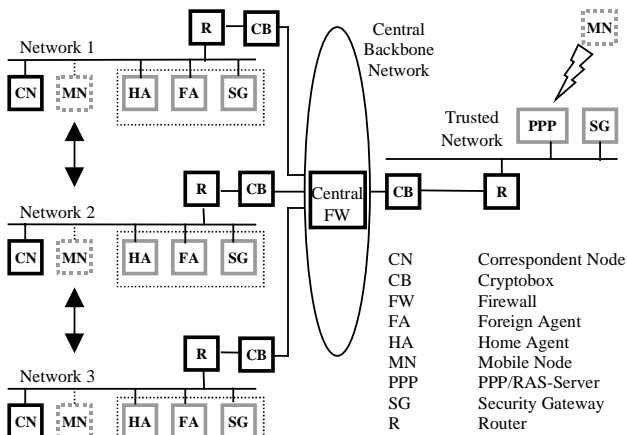
The first step of the deployment of the mobility enhancements into the existing network infrastructure consists of extending the individual authorities with separate subnets which at first play the role of the authority network. These subnets are equipped with the appropriate mobility agents and security gateways. Likewise the central firewall is extended with a separate IPsec firewall which in a later operational stage should merge with the central firewall. The purpose of such a ‘co-located’ scenario is to be able to use the real network environment (which involves different network components like an ATM backbone, edge devices, crypto modules, etc.) during installation and tests and later ensure a smooth transition into an operational mode.

## 2.2. The Secure Mobile IP Enhanced Intranet

To support the desired mobility functions each of the 3 participating departmental networks had to provide mobility agent functionality with all of the mobility agents acting also as IPsec firewalls. The central firewall was extended by a co-located additional firewall system supporting the mobility specific communication. In detail we have the following components:

- Each involved network was extended by mobility agents according to Mobile IP, which implement the Home Agent (HA) and Foreign Agent (FA) functionality. Here the public domain Mobile IP software package from Dynamics [10] was used.
- The selected mobile computers (Windows NT) were equipped with appropriate mobility software modules (NDIS intermediate driver), whereby they became Mobile Nodes (MN) in terms of Mobile IP. MN software from RoamIn [11] (public domain) was used.
- In order to support strong authentication as proposed by IPsec each network involved was equipped with a dedicated Linux OS FreeS/WAN [9] firewall (fw) which is available as public domain software. These IPsec modules perform authentication [10] of the Mobile IP traffic and can also be placed with the agent modules on the same host.
- A central Linux OS FreeS/WAN based firewall host (FW) was assigned to the already existing central firewall system to allow Mobile IP data streams to bypass the central firewall and to enable their central control.

An overview of the present physical environment is given in the following picture:



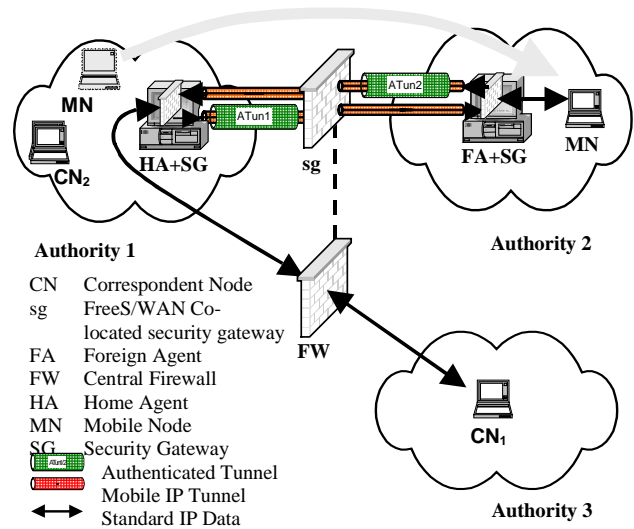
**Figure 2: Physical Structure of Mobile IP Test Environment**

The environment described here allows a mobile node to move seamlessly between different authorities inside of the governmental organization, but not outside. The only way to get access to an authority subnet from the outside is provided by a remote access dial-up server which supports CHAP protected access.

Communication relations between a mobile host, which is located in its home network and any other host in his home network are not affected by this concept, since the communication takes place without participation of Mobile IP. If in contrast a mobile node is situated in a foreign network, two basic scenarios must be distinguished. For details see Figure 1.

1. The Correspondent Node (CN) is in a third network (CN<sub>1</sub>), i.e. CN<sub>1</sub> is neither in the home network of the MN nor in the foreign network of the MN. In this case the communication between CN<sub>1</sub> and MN will be routed over the central firewall where the traffic is controllable according to the current policies. Mandatory in this case is that the respective HA only routes those packets to the MN which had been already controlled by the local security gateway (fw). This is done via authentication of the Mobile IP tunnel by the security gateway (fw). For the reverse communication direction from the MN to CN<sub>1</sub> the packets can go directly via the central security gateway (FW) by means of standard IP routing. In this case the FW is required not to perform ingress filtering. Otherwise reverse tunneling is required to allow firewall traversal.
2. If the CN is located in the MN's home network (CN<sub>2</sub>) and the MN is away, all outgoing and

incoming packets between CN<sub>2</sub> and MN will not be routed over the central firewall (in case of reverse tunneling) which violates the assumption that all traffic crossing authority boundaries has to be controlled by FW. But in this case both nodes, CN<sub>2</sub> and MN, stem from a common home network. Insofar this situation corresponds to the Mobile IP paradigm as it concerns communication between 2 hosts, which originate from the same home network and would also not be subject to an appropriate check by FW, if the MN was in its home network.



**Figure 3: Secure Mobile IP Communication Between Different Authorities**

The described implementation assumes the Home Agent to be a trusted host, so that it is guaranteed that for the CN-MN connection (first scenario) only packets are tunneled which were already controlled by the central firewall FW. Likewise for the second scenario where two hosts with a common home network perform a 'virtually internal' communication, the HA is assumed to operate as a trusted host to fulfill the security requirements. In case of reverse tunneling the involved FA is also required to act as a trusted host for the same reason.

As a consequence thereof the authentication of the Mobile IP tunnels has become indispensable. For providing this authentication functionality additional security gateways along the path of the Mobile IP tunnels were required. In order to allow the control of all packet streams at the central firewall the authenticated tunnels are terminated at the firewall's co-located security gateway.

### 3. Summary and Conclusions

The present prototype implementation shows how VPN technology can be used to protect mobile nodes roaming beyond the boundaries of their home networks of an individual organizational intranet.

As a basic security measure all publicly accessible network points of attachment (and foreign agents as well) are placed outside the authorities firewall, i.e. in the DMZ. This precaution provides strong protection for the private networks from unauthorized parties. At the same time this measure allows visitors of the foreign authority to connect to the network and access their home authority network without compromising the private network's security. This in turn required the deployment of VPN technology by which authorized mobile nodes can traverse the firewalls without exposing the mobile nodes or the authority networks to additional security threats.

In order to allow control of authorized mobile nodes all traffic originating from the agents has been authenticated using IPsec Authentication Header.

It has been demonstrated that such scenario can be accomplished with the deployment of public domain software. Linux based software by Dynamics was used for the provision of Mobile IP agents, Windows NT based RoamIn software yielded the mobile node component, and FreeS/WAN's IPsec implementation added the necessary authentication procedures.

---

[1] W. Simpson (Editor), "The Point-to-Point Protocol (PPP)", *IETF STD 51*, July 1994, ([www.ietf.org/rfc/rfc1661.txt?number=1661](http://www.ietf.org/rfc/rfc1661.txt?number=1661))

[2] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, "Address Allocation for Private Internets", *IETF RFC 1918*, February 1996, ([www.ietf.org/rfc/rfc1918.txt?number=1918](http://www.ietf.org/rfc/rfc1918.txt?number=1918))

[3] [W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", *IETF RFC 1994*, August 1994, ([www.ietf.org/rfc/rfc1994.txt?number=1994](http://www.ietf.org/rfc/rfc1994.txt?number=1994))

[4] C. Perkins (Editor), "IP Mobility Support", *IETF RFC 2002*, October 1996, ([www.ietf.org/rfc/rfc2002.txt?number=2002](http://www.ietf.org/rfc/rfc2002.txt?number=2002))

[5] C. Perkins, RFC 2003 "IP-in-IP", *IETF RFC 2003*, Oktober 1996, ([www.ietf.org/rfc/rfc2003.txt?number=2003](http://www.ietf.org/rfc/rfc2003.txt?number=2003))

[6] S. Kent, R. Atkinson, "Security Architecture for the Internet", *IETF RFC 2401*, November 1998, ([www.ietf.org/rfc/rfc2401.txt?number=2401](http://www.ietf.org/rfc/rfc2401.txt?number=2401))

---

[7] S. Kent, R. Atkinson, "IP Authentication Header", *IETF RFC 2402*, November 1998, ([www.ietf.org/rfc/rfc2402.txt?number=2402](http://www.ietf.org/rfc/rfc2402.txt?number=2402))

[8] R. Thayer, N. Doraswamy, R. Glenn., "IP Security Document Roadmap", *IETF RFC 2411*, November 1998, ([www.ietf.org/rfc/rfc2411.txt?number=2411](http://www.ietf.org/rfc/rfc2411.txt?number=2411))

[9] IPsec Software, *FreeS/WAN Homepage*: [www.xs4all.nl/~freeswan/](http://www.xs4all.nl/~freeswan/), FreeS/WAN Mailing List: [linux-ipsec@clinet.fi](mailto:linux-ipsec@clinet.fi), Mailing List Archive [www.sandelman.ottawa.on.ca/linux-ipsec/](http://www.sandelman.ottawa.on.ca/linux-ipsec/)

[10] Mobile IP Agent (Server) Software, *Dynamics Homepage*: Helsinki University of Technology, TSE Institute, ([www.cs.hut.fi/Research/Dynamics/](http://www.cs.hut.fi/Research/Dynamics/)), software source: [dynamics-0.7.1.tar.gz](http://dynamics-0.7.1.tar.gz)

[11] Mobile IP Node (Client) Software, *GMD FOKUS*, [www.roamin.com](http://www.roamin.com)