



**INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH
TECHNOLOGY**

VIRTUAL PRIVATE NETWORKING MOBILE COMPUTING

Ammar Es-Said, Labriji El Houssine, Hanoune Mostafa, Ghanimi Fadwa

University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco, Department of Mathematics and Computer

University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco, Department of Mathematics and Computer

University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco, Department of Mathematics and Computer

University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco, Department of Mathematics and Computer

ABSTRACT

In mobile communications systems, mobile units are free to move at a local, regional, national level, track international, while providing communication. With the increasing use, mobile users wish to increasingly access Internet services during their travels, the opportunities offered by these technologies has given rise to a new paradigm "«mobile computing »

This paradigm underlying the concept of availability or presence "in any place and at any time" certainly such mobility involves Internet and wireless technologies in a process to provide advanced services to nomadic users, however in order to be able to offer these services with satisfactory quality, you must face many challenges in relation to the reliability of services infrastructure, energy efficiency of mobile devices.

KEYWORDS: Mobility, VPN, mobile computing, mobile security, Wireless technologies

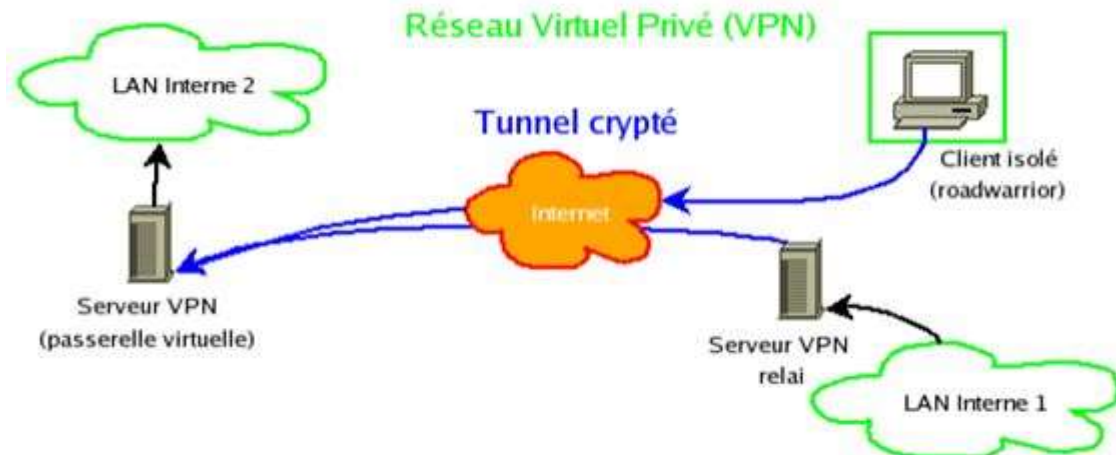
INTRODUCTION

With the growing use of various mobile devices, mobile users have more need for accessing internet services during their travels. The opportunities these technologies have given rise to a new paradigm: one of the major causes of serious data loss, after attacks and viruses computer is the loss and theft of mobile devices, is so potentially a high risk of disclosure of confidential information, mobility therefore poses the problem of the security of data in a very acute, resolve it by the enactment of unpleasant constraints, or sometimes downright unrealistic.

PRIVATE VIRTUAL NETWORKING

In the field of communications networks can be defined mobility as the ability to access all of the services, but on the internet we know where spend data because paths change, these data can therefore be listened to or intercepted





But then why private virtual network? the data are encrypted and that only two networks are but are not seen from the outside so the relationship of securely at very low cost by a simple connection but this is done at the expense of performance because the passage through a dedicated link.

THE FUNCTIONING OF THE VPN

We can say that the VPN is only a concept, this is not an implementation, it is characterized by:

- Encryption of the tunnel: the data exchanged on the Internet must be duly encrypted between the VPN client and the VPN server.
- Management addresses: all users must have a private address and the new client to get one easily.
- The encryption keys must be regenerated often (automatically).

→ Les réseaux mobiles sans fil, peuvent être catégorisés en deux classes : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire, et les réseaux sans infrastructure ou les réseaux ad hoc :

- In a cellular network, the territory covered, or the coverage area is generally divided into small geographically limited areas, they are presented by hexagons, in this section, we present the Sub radio systems and network that make up this architecture as well as some consideration that determine the size of the cells.
- An ad hoc network can be defined as a collection of mobile entities interconnected by wireless technology forming a temporary network without using any administration or support fixed., no assumption or limitation is made on the size of the network, theoretically, it is possible that the network has a very high size.

THE BASIC REQUIREMENTS OF MOBILE VIRTUAL PRIVATE NETWORK

To ensure the confidentiality and integrity of data as it passes over the Internet, measures and security mechanisms are also used to ensure the transfer of these data mobile safely through a medium non-secure, one of the most important security mechanisms

- Authentication which means checking the equipment of the user or the user's identity.

Equipment authentication : allows you to restrict access to provide credentials from a remote VPN device.

User authentication : check if a connection by using specific equipment, where the user must provide a user name and a password. This password may be a static password or an instant password.

- Data encryption is the process of modifying the data in a format can be read the message, the recipient of the data must have the correct decryption key, data encryption is used to resolve the problems of listening.



MOBILE SECURITY AND VIRTUAL PRIVATE NETWORKING



The solution proposed to provide a better securing mobile data by extending the perimeter secured to moving parts, this can be done more often with a VPN which is that the mobile device, wherever he is, is considered as part of the protected cell, the level of the highest possible security of authentication technologies, data crossing are protected against access.

- Improve productivity by extending the network and applications
- Reduce communication costs and increase flexibility.

CONCLUSION

Mobility has become over time a true philosophy of life, so it makes the redefinition, the absence of a central management of the capabilities currently are not designed for such an environment (dynamic), they do not take into account resource constraint because not only the environment is dynamic, but resources are also limited what further complicates the problems, because it is well known that security solutions are intensive in terms of resources, however because of the importance it is necessary to meet the challenge, because designing a foolproof security for mobile networks mechanism is necessary.

REFERENCES

1. Abderrezak Rachedi Contributions à la sécurité dans les réseaux mobiles ad Hoc. Networking and Internet Architecture , 2008.
2. SAMUEL PIERRE Réseaux et systèmes informatiques mobiles : Fondements, architectures et applications Relié – 5 avril 2003 (4_5).
3. Abderrezak Rachedi Contributions à la sécurité dans les réseaux mobiles ad Hoc. Networking and Internet Architecture, 2008.
4. Abdelmajid HAJAMI Sécurité du routage dans les réseaux sans fil spontanés : cas du protocole OLSR 12 Mai 2011 (2).
5. Djedjiga BENZID le réseau privé virtuel (vpn) sur les réseaux maillés sans fil wmn LE 11 MARS 2014 (25_28).
6. ShareVB Sécurité GNU/LINUX Virtual private Network (1_2) .Jadwiga Indulska and Peter Sutton, Location management in pervasivesystems, Proceedings of the Australasian information security workshop, vol. 21, 2003,pp. 143–151.
7. Shanshan Jiang, Svein Hallsteinsen, Paolo Barone, Alessandro Mamelli,Stephan Mehlhase, Ulrich Scholz, Frank Eliassen, and Rudiger Kapitza,Hosting and using services with qos guarantee in self-adaptive servicesystems, vol. 6115, pp. 15–28, Springer Berlin / Heidelberg, 2010.
8. Konstantinos Kakousis, Nearchos Paspallis, and George Angelos Papadopoulos,A survey of software adaptation in mobile and ubiquitous computing, Enterprise Information Systems 4 (2010), no. 4, 355–389.
9. Yoann Maurel, Ada Diaconescu, and Philippe Lalanda, Ceylon : A serviceoriented framework for building autonomic managers, Engineering of Autonomic and Autonomous Systems, IEEE International Workshop on 0 (2010),3–11.