Contemporary Engineering Sciences, Vol. 6, 2013, no. 3, 135 - 142
HIKARI Ltd, www.m-hikari.com

Conception and Implementation of Centralized and Dynamic VPN Services

Sanaa Difaa

Université Hasan II_Mohammedia, Faculte des Sciences de Casa
Sdifaa1@yahoo.fr

Mohamed Azouazi

Université Hasan II_Mohammedia, Faculte des Sciences de Casa
azouazii@hotmail.com

Abstract

In information technology, trying to define virtualization as a set of technical hardware and / or software that can run on a single machine multiple operating systems and / or multiple applications separately from each other, as if they operated on separate physical machines.
The approach to maximize resources on a single platform using virtual machines has been proven.
In this paper we study the design and implementation of VPN services in a centralized way to manage and secure these services

Keywords: VPN, IPSec, PPTP, L2F, L2TP, VNOC, S.CVPN

I. Introduction

Virtualization tools used to run what is commonly called virtual private servers (VPS or Virtual Private Servers) or virtual environments (VE and Virtual Environments)

The word is also used virtualization for client servers. It is commonplace in this case the position that connects to servers.
Virtualization is useful in many areas of computing

1. Modelling of computer network.
2. Production use.
3. Allows to continue to run old applications or devices over recent UC.

II. Principle of virtualization

1. Modelling of computer network

Virtualization allows from a machine with at least 2 G of RAM and a hard drive capacity correctly (the size of virtual disks can be dynamic) and increases only as and when required, create virtual machines do not necessarily using the same base OS and can operate in the same network environment, thus can model for example a DHCP server with machines that connect to it.

2. Production use

Holders in companies who manage multiple production servers (domain controller, mail, dhcp, sql server etc ...), will be able to integrate all these servers into one or better two powerful systems that will virtualize older servers.
All this by reducing noise, dissipating heat and energy bills and providing server consolidation, greater availability of services and adapting to new business solutions easy to implement on new virtual servers.

3. Maintaining legacy systems and devices

Virtualization provides the ability to deploy, move or clone an application from one platform to another in a network, including during operation. Migration of applications in operation, with the responsiveness and this scale requires new levels of performance, reliability and standardization of networks.
This explains why careful planning network architectures is an initial step of a virtualization process realy creates value.

Interests of virtualization:

- Optimal use of resources of machinery (distribution of virtual machines on physical machines based on the respective charges)
- Installation, deployment and easy migration of virtual machines from one physical machine to another, especially in the context of a production from a qualification environmental or from pre-production, easy delivery, saving hardware by pooling (power consumption, physical maintenance, monitoring, support, hardware compatibility, etc.)

III.Case Study:

1. **Problematic**

Often companies feel the need to communicate with affiliates, customers or even staff who are geographically remote via Internet for real-time processing of secure electronic transactions

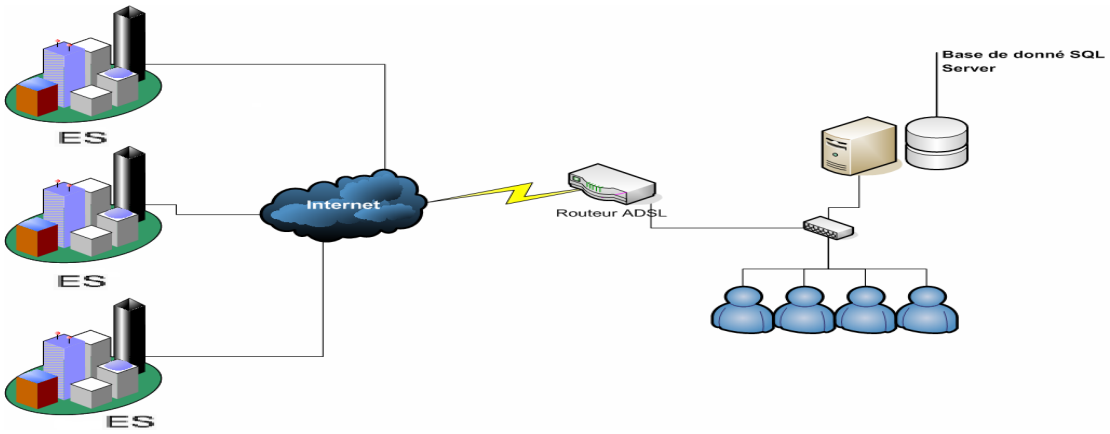

Figure 1: The initial architecture

Data transmitted over the Internet is much more vulnerable than when running on an internal network in an organization, which means that data borrows a public network infrastructure belonging to different operators.
This network is listened to by an indiscreet user or even hijacked. It is not conceivable to transmit under such conditions sensitive information to the organization or company.
So we will need to obtain a secure and reliable connection cost and easy to configure

2. solution

A good compromise is to use the Internet as the transmission medium using a protocol encapsulation (tunneling in English, which sometimes misuses the term "tunneling"), that is to say, encapsulating the data to be transmitted encrypted. This is known as virtual private network VPN
The VPN system therefore provides a secure connection at a lower cost. A virtual private network is based on a protocol called tunneling protocol (tunneling), that is to say, a protocol that allows data from one end to the other of the VPN to be secured by cryptography algorithms.
The term "tunnel" is used to symbolize the fact that between the input and output data is encrypted VPN (encrypted) and therefore incomprehensible for anyone between both ends of the VPN, as if the data passed in tunnel. In the case of a VPN established between two machines, called the element VPN client to encrypt and decrypt data on the user side (client) and VPN server.

Tunneling protocols

- major tunneling protocols are:

PPTP (Point-to-Point Tunneling Protocol) is a protocol developed by Microsoft level2, 3Com, Ascend, U.S. Robotics and ECI Telematics.

- L2F (Layer Two Forwarding) is a protocol developed by Cisco level2, Northern Telecom and Shiva. It is now almost obsolete
- L2TP (Layer Two Tunneling Protocol) is the culmination of work to converge the features of PPTP and L2F. It is thus a Level 2 protocol based on PPP.
- IPSec (Internet Protocol Security) is a set of protocols (OSI Layer 3) using algorithms to secure data transport over an IP network.

So IPSec is a protocol used to secure communications at the network layer. This is actually a protocol providing improvements in security to IP to ensure the confidentiality, integrity and authentication exchanges.

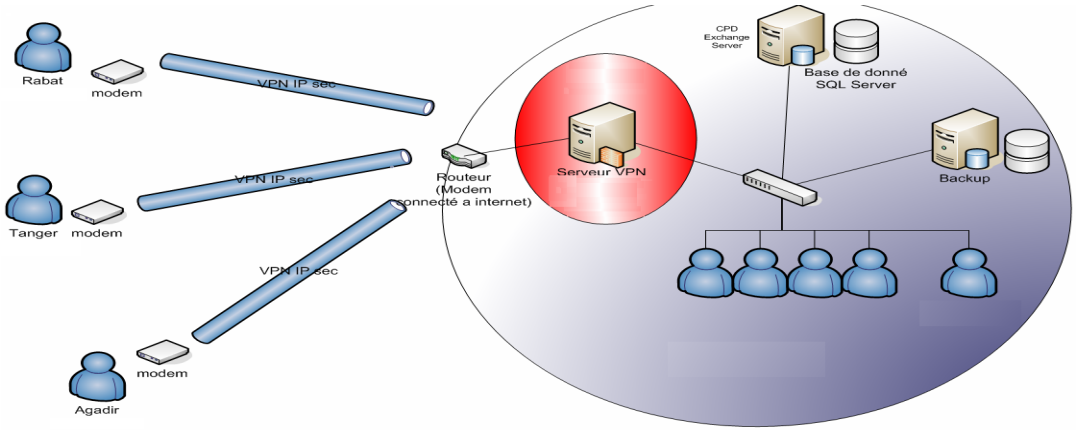

Figure 2: VPN Solution proposed

IV. Improvement of the proposed solution

We defined an architecture based VPN IPsec tunnels between distributed sites on the Internet, these sites can be a LAN, a line of business, a partner network, or even a user. VPNs are dynamic and their topology depends on the addition or removal of a site VPN.

All services (authentication sites, adding and removing a site configuration) are actually dynamic.

This solution is based on a new entity, the operator VPN. It operates a center of operation, VNOC (or Virtual Network Operation Center) that configures remote VPN sites dynamically, depending on user needs.

A second key aspect of this architecture is its centralized nature, necessary to apply policies to all sites consistently. Central administration or VNOC (Virtual

Network Operation Center), supports the implementation of policies VPNs VPN gateways (or Edge Device, ED) sites. ED is one for each VPN site and is the point of entry and exit tunnels VPNs on the website. The EDs play an active role in this architecture: in particular, they send requests to participate in VNOC or leave a VPN. Thus, if an ED request to participate in a VPN, and if the site of the ED is authorized, the VNOC sends back the necessary configuration files. The VNOC also informs other EDs concerned by this to establish VPN tunnels, and all communications site-to-site IPsec are then secured.
To summarize the characteristics of this approach:

- independence vis-à-vis ISPs: This service can be applied among sites related to different ISPs (accèsInternet providers).
- Centralized approach: the presence of a center of administration facilitates the control and configuration of VPNs and control services accounting and billing.
- Use of standard bricks: the traffic between sites is protected by IPsec VPNs, and traffic between VPN sites and VNOC.
- Dynamic approach: each site sends queries dynamically at VNOC to attend or leave a VPN, depending on the needs of users, and VNOC immediately updates the VPN configuration.
- Several topologies are possible for communications site-to-site: in this article only in stars VPNs are considered, however, other topologies are possible. Services group communication (multicast) are also possible.
- Administration: the Authentication and access control are performed by the users VNOC which also offers a tool for configuration and monitoring of VPNs.
- Operational Solution: end this approach is fully implemented and available commercially.

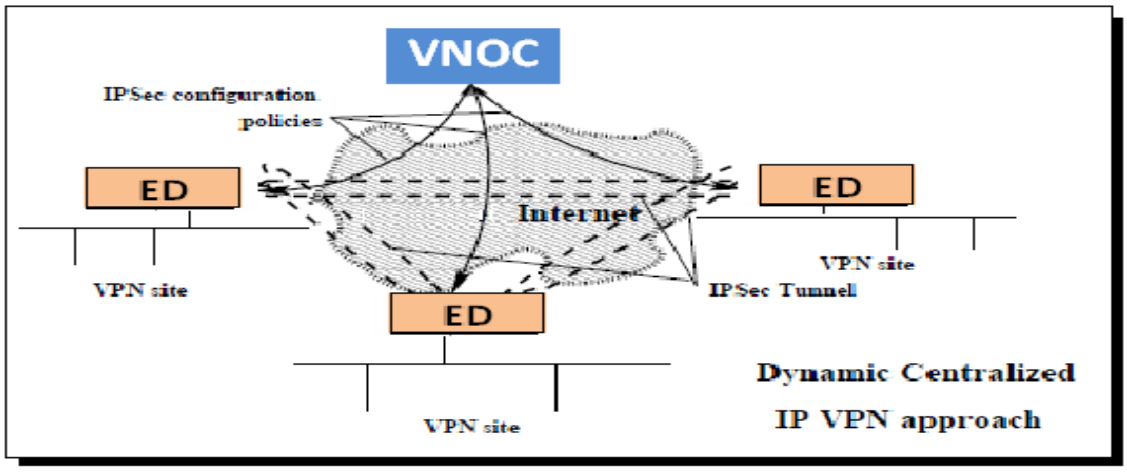

Figure 3: Centralized approach and dynamic VPN (site to site case).

Centralized management, provides authentication and authorization of clients, policy management, and configuration of security tunnels. Which meets the security criteria.
Finally, server virtualization allows much greater success in load distribution and reconfiguration of servers in case of changes or temporary failure (emergency plan, etc.).

V. Experimentation:

1. Carried out Transactions in function of time before improvement:

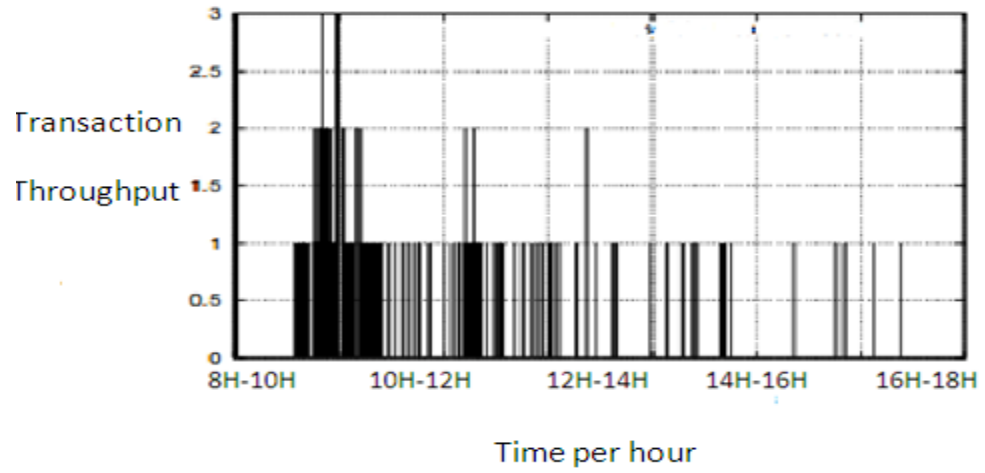

Figure 4: Variation of the flow of transaction depending on the time before

2. Carried out Transactions in function of time after the upgrade:

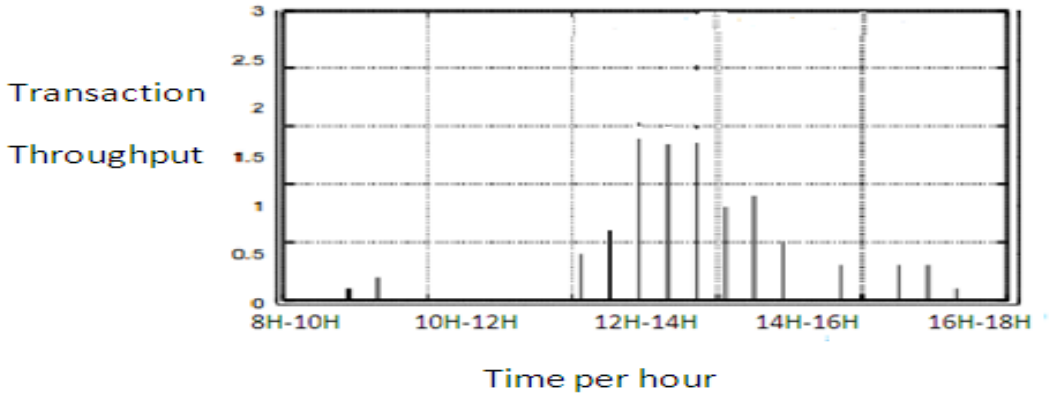

Figure 5: Variation of the flow of transaction depending on the time after

VI. Conclusion

The virtualization approach fully justifies the upgrade performance and reliability of enterprise networks, but self- sufficient in itself. Updated and optimized

networks bring to the company the advantage of integrating the latest technologies, but also release significant capacity for the company:

- stay in the race, with networks that allow to have basic services, have a reliable basis, and able to support business users to meet the requirements set by the regulators, and satisfy customers;
- overtake the competition with technologies that improve productivity, reduce costs and overcome your competitors by forcing a permanent confrontation to keep up with your level;
- reverse the play, through innovative technologies to create new services that will redefine the competitive environment.

It is, ultimately, to create a network capable of supporting these objectives, to better ensure the quality of your service and your availability commitments and overtake the most demanding needs of tomorrow's business.

References

[1] SECURITY ARCHITECTURE FOR THE INTERNET PROTOCOL Novembre 1998 RFC 2401 S. Kent, R.Atkinson
[2] REQUIREMENTS FOR IPSEC REMOTE ACCESS SCENARIOS Mars 2002 draft-ietf-ipsra-reqmts-05 S. Kelly, S.Ramamoorthi
[3] DEMYSTIFYING THE IPSEC PUZZLE 2001 S. Frankel Artech House
[4] IPSEC SECURING VPNS 2001 C.R. Davis RSA Press
[5] B. Gleeson. Uses of IPsec with Provider Provisioned VPNs. PPVPN Working Group, August 2001. draft-gleeson-ipsec-ppvpn-00.txt, work in progress.
[6] Check Point Software Technologies Ltd. IPSec Versus Clientless VPNs for Remote Access, September 2002. white paper, http://www.checkpoint.com.
[7] Cisco Secure VPN Client Solutions Guide, 2002. Cisco Systems Inc., Number: OL-0259-02.
[8] G. Laporte,G. et I.H. Osman, Routing problems : A Bibliography, Annals of Operations Research, 1995
[9] G.Laporte , M. Potvin, J.Y et F. Semet , Classical and modern heuristics for the vehicle routing problem, International Transactions in Operational Research, 2000
[10] DHCPV4 CONFIGURATION OF IPSEC TUNNEL MODE Juillet 2001 draft-ietf-ipsec-dhcp-13 B. Patel, B. Aboba, S. Kelly, V. Gupta
[11] PIC, A PRE-IKE CREDENTIAL PROVISIONING PROTOCOL Février 2002 draft-ietf-ipsra-pic-05 Y. Sheffer, H. Krawczyk, B. Aboba
[12] SECURING L2TP USING IPSEC Novembre 2001 RFC 3193 B.Patel, B. Aboba, W.Dixon, G.Zorn, S.Booth
[13] IPSEC AND L2TP IMPLEMENTATION IN WINDOWS 2000 3 Août 2000 Support Technique Microsoft (Q265112
[14] G. Laporte, Y. Nobert : An exact algorithms for the vehicle routing problem. Networks, 14, n°1, pp. 161-172, 1984

[15] J.K. Lenstra and A.H.G Rinnoy Kan : Complexity of vehicle routing and scheduling problems. Networks, 11 : 221-227, 1981
[16] M.Dorigo, L.Maria Gambardella. Ant colony system : A cooperative Learning. Approch to the travelling Salesman Problem. IEEE Transactions on Evolutionary Computation, Vol.1, No.1, 1997
[17] P. Blaise : Tournées de véhicules d'une société coopérative: algorithmes séquentiels et parallèles:
http://www.prism.uvsq.fr/rapports/1996/document_1996_6.ps.
[18] P. Knight, H. Ould-Brahim, and B. Gleeson. Network based IP VPN Architecture using Virtual Routers. L3VPN Working Group, April 2004. draft-gleeson-ipsec-ppvpn-00.txt,work in progress.
[19] V Cerf et R Kahn. A Protocol for Packet Network Intercommunication. IEEE Transactions on Communications, 22(5):637– 648, Jan 1974.

Received: February 15, 2013