Proceedings in MANUFACTURING SYSTEMS

Proceedings in Manufacturing Systems, Volume 7, Issue 1, 2012 ISSN 2067-9238

THE ENTERPRISE IPSEC VPN SOLUTIONS

Sebastian Marius ROŞU[1], Marian Marius POPESCU[2], George DRĂGOI[3,*]
Liviu Mihail MATEESCU[4], Ioana Raluca GUICĂ[5]

[1)] PhD, Special Telecommunications Service, Radio Communications Department, Bucharest, Romania
[2)] PhD Student, Special Telecommunications Service, Information Technology Department, Bucharest, Romania
[3)] Prof., PhD, Faculty of Engineering in Foreign Languages, University "Politehnica" of Bucharest, Bucharest, Romania
[4)] Lecturer, Economics Department, University "Politehnica" of Bucharest, Bucharest, Romania
PhD Student, Faculty of Engineering in Foreign Languages, University "Politehnica" of Bucharest, Bucharest, Romania

Abstract: *Now, in the 21st century, all enterprise have a local area network, a virtual private network, an Intranet and Internet, servers and workstations for operations, administration and management working together for the same objective: profits. Internet Protocol Security is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network. This work analyses the network architecture for an enterprise geographically dispersed.*

Key words: *virtual enterprise, virtual enterprise network, IPSec, virtual teams, network architecture..*

1. INTRODUCTION

The optimization of product benefit must be the focus of all network activities [1]. The work comprises components for integration of information systems, visualization of the planning and production situation, communication to enable cooperative decision making under uncertainty, optimization of plans and simulation of the decisions, network diagnostics and performance monitoring among others [2]. This involves a number of challenges such as providing members access to network-wide real time information, enable visualization of the available information, secure the interaction between advanced ICT based decision support tools and human decision making, and creating a coordinated and collaborative environment [1] for planning and decision making. Distributed processing offers the most general, flexible and promising approach for the provision of computing services [3]. Monitoring of such process execution may allow the manager to detect faults and guarantee correct execution [4]. Because the new communication system enables many more interactions between many more participants, it has security requirements beyond the conventional confidentiality, integrity and availability properties provided by conventional security systems [5].

Development of information technology and communication has led to widespread deployment of technical solutions for [6]: accessing and processing data and information, the transmission of data and information in a network environment with distributed destinations, connect different users regardless of their geographical distance and position. The complexity of the human enterprise continues to grow at an accelerating pace as larger numbers of people take on increasingly ambitious tasks in a world that grows in size, complexity, and constraining factors [7]. As a general requirement for an infrastructure support is than the enterprises must be able to inter-operate and exchange information's and knowledge in real time so that they can work as a single integrated unit, although keeping their independence/autonomy [6]. For the future, e-services and e-business, as were defined, require the enterprise re-thinking and re-modeling, with the sys-tem and applications design for an efficient use of new network technologies [8]. While many of the currently deployed m-commerce systems already allow users to access e-commerce services while on the move, the increasing complex characteristics of m-commerce systems is beginning to stretch the traditional relationship between user and machine [9]. Various network services can be used by everyone, either supplying or demanding them. A large range of distribution, the platform independence, an big number of user friendly services that are easily accessible through the World Wide Web as well as the open standards used and free or budget-priced products (such as browsers, html editors, software updates) have lead to a high and continuously growing proliferation of the Internet [10]. Development of ICT leaves much more freedom to the designers and consultants to accommodate organizations to other influences, both internal and external [11]. Enterprises are now facing growing global competition and the continual success in the marketplace depends very much on how efficient and effective the companies are able to respond to customer demands [12]. Starting from these considerations, this work analyzed the network architecture for an enterprise geographic dispersed as support for virtual private net-

[*] Corresponding author: 313 Splaiul Independenţei, Sector 6, Bucharest, 060042, Romania
Tel.: 004021 402 0759
E-mail addresses: *gdragoi@mix.mmi.pub.ro , Dragoi.george23@gmail.com, office@sebastianrosu.ro, sebastianrosu@stsnet.ro, marius.popescu@stsnet.ro, mateescu_liviumihail@yahoo.com, guicaioana@zahoo.com*

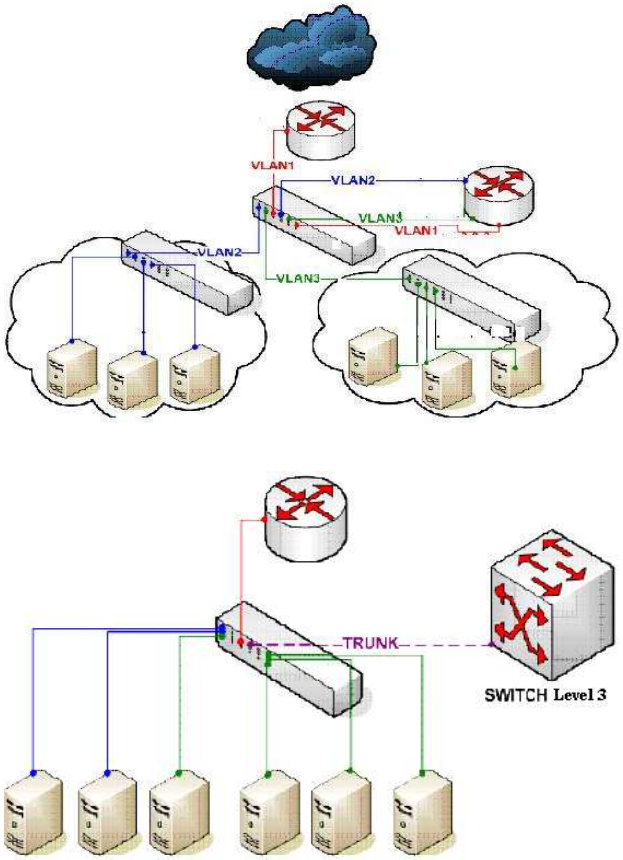

Fig. 1. Virtual Private Network solutions today.

works (VPNs) possible structures (based on Internet Protocol Security – IPSec).

2. VIRTUAL ENTERPRISE BUSINESS NETWORK

Appearance of virtual networks is related to the evolution switches (see Fig. 1).

A virtual enterprise business network (VEBN) target is to combine a group of users regardless of their geographical position but such a manner that it flows together and to provide the best performance. The second advantage of a virtual network consists of administrative solutions which accompany the products, allowing users moving from one group to another through a simple reconfiguration of the equipment. The basic idea behind a virtual enterprise network is to establish a dynamic organization by the synergetic combination of dissimilar companies with different core competencies, thereby establishing a best of everything consortium of enterprise geographically dispersed to perform a given business project and to achieve maximum degree of customer satisfaction. In this emerging business model of virtual enterprise network, the decision support functionality, which addresses the issues such as selection of business partners, coordination in the distribution of production processes and the prediction of production problems, is an important domain to be studied. A virtual enterprise network (see Fig. 2) needs its own Private Member Collaboration System to communicate and develop its projects and bids. In this context, the virtual team concept is used to cover a wide range of activities and forms of technology-supported working. Virtual team is a group of people who interact

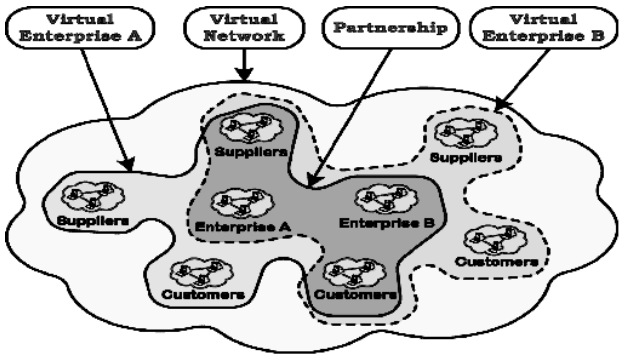

Fig. 2. Virtual Enterprise Business Network view.

through interdependent tasks guided by common purpose and work across links strengthened by information, communication and transport technologies.

With rare exceptions all organizational teams are virtually to some extent. This era is growing popularity for virtual team structures in organizations. Virtual teams are the teams whose members use technology to vary degrees in working across location, temporal, and relational boundaries to accomplish an interdependent task. Enterprise virtual team's members are located in more than one physical location. This team trait has fostered extensive use of a variety of forms of computer-mediated communication that enable geographically dispersed members to coordinate their individual efforts and inputs. Also, virtual teams can be defined as groups of workers geographically, organizationally and/or time dispersed brought together by information technologies to accomplish one or more organization tasks. The degree of geographic dispersion within a virtual team can vary widely from having one member located in a different location than the rest of the team to having each member located in a different country. The availability of a flexible and configurable base infrastructure is one of the main benefits of virtual team's works in a virtual enterprise business network environment. Where are the advantages of VEBN solutions in the new digital economy? Firstly, a VEBN is necessary to combine a group of users regardless of their geographical position but such a manner that it flows together and to provide the best performance.

Secondly, the advantage of a VEBN consists of simple administrative solutions which accompany the products, allowing users moving from one group to another group through a reconfiguration of the network equipments.

3. ENTERPRISE NETWORK ARCHITECTURE

An enterprise network consists of a group (departmental, interdepartmental, etc.) of local area networks (LANs), located in the same place or geographically dispersed, interconnected using wide area networks (WANs) and contains a number of inter-networking devices (e.g. switches, routers, gateways, etc.) which is under the control of the organization or a telecommunication company. A communications network forms the backbone of any successful organization [13].

Metropolitan networks play a critical role in the overall expansion of network services because they not only provide for services within individual metropolitan areas, but they also serve as the gateways for wide-area nation-

al- and international-scale networks [14]. In an enterprise network, a large number of nodes are interconnected together through a computer network as follow [15]:

- *End-user nodes* represented by access points such as workstations, personal computers, printers, mainframe computers, etc.
- *Network active elements* consist of devices such as multiplexers, hubs, switches, routers, and gateways; the active elements and links provide the needed physical communication paths between every pair of end-user nodes.

Traditional infrastructures type Internet/Intranet/ Extranet have now a fast dynamic, marking the transition to new generation networks to provide higher speeds to the user (end to end), for different types of transactions and a reduction in the number of servers by passing information between two nodes [12, 16].

The trend toward IP-based transport infrastructures for all real-time and non-real-time applications opens the door for a new paradigm in integrated voice and data communications.

A hierarchical network design model breaks the complex problem of network design into smaller, more manageable problems [16, 17]. An important step in designing an enterprise network is to define a network perimeter. The enterprise network perimeter defines a security layer complemented with other security mechanism [18, 19]. Communications within and outside the enterprise perimeter must be through a traffic control point - provided by firewalls and other security devices [16].

Various network services can be used by everyone, either supplying or demanding them. A large range of distribution, the platform independence, an big number of user friendly services that are easily accessible through the World Wide Web as well as the open standards used and free or budget-priced products (such as browsers, html editors, software updates) have lead to a high and continuously growing proliferation of the Internet [20]. However, the application-to-application communication problem still exists. Businesses have needed a standardized way for applications to communicate with one another over networks; no matter how those applications were originally implemented [21].

Appearance of virtual networks is related to the evolution switches (see figure 1). A *virtual network* solution is used to combine a group of users regardless of their geographical position but such a manner that it flows together and to provide the best performance.

The basic advantage of a virtual private network consists of administrative solutions which accompany the products, allowing users moving from one group to another through a simple reconfiguration of the equipment [22]. In fact, by definition, a virtual local network is a logical grouping of local network components without regard to their physical grouping.

The *virtual private network* (VPN) is a network emulated (the *virtual*) built on public infrastructure (*shared*), dedicated to a client (the *private*) to connect users in locations and to ensure similar conditions of integrity, confidentiality and quality similar with those of a private network. VPNs allows the provisioning of private network services for an organization or organizations over a public or shared infrastructure such as the Internet or service provider backbone network.

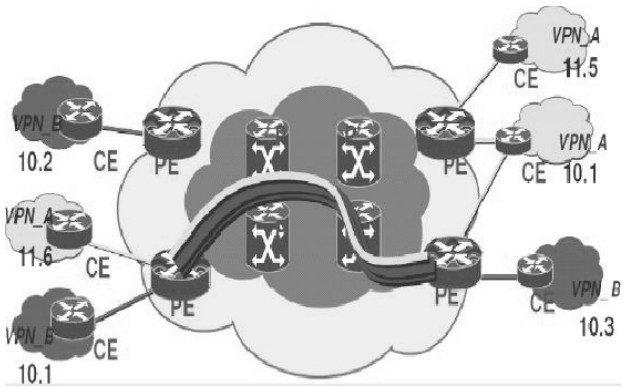

Fig. 3. VPN IP by MPLS.

The shared service provider backbone network is known as the VPN backbone and is used to transport traffic for multiple VPNs, as well as possibly non-VPN traffic. VPNs provisioned using technologies such as Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits (VC) have been available for a long time, but over the past few years IP and IP/Multiprotocol Label Switching (MPLS) – based VPNs have become more and more popular (see Fig. 3).

VPNs may be service provider or customer provisioned and fall into one of two broad categories: site-to-site VPNs connect the geographically dispersed sites of an organization or organizations and remote access VPNs connect mobile or home-based users to an organization's [18, 23]. A VPN solution typically requires integration of several services (design, network management services, dial-up or dedicated access).

IPsec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network (VPN). IPSec Tunnel mode is used to secure gateway-to-gateway traffic. IPSec Tunnel mode is used when the final destination of the data packet is different from the security termination point.

IPsec Tunnel mode protects the entire contents of the tunneled packets. The IPSec Tunnel mode data packets sent from the source device are accepted by the security gateway (a router or a server) and forwarded to the other end of the tunnel, where the original packets are extracted and then forwarded to their final destination device. IPSec tunnel is usually built to connect two or more remote LANs via Internet so that hosts in different remote LANs are able to communicate with each other as if they are all in the same LAN. Common commands to create an IPSec tunnel (for Cisco® equipments) are presented in Fig. 4 (connects Enterprise headquarter LAN through an IPSec tunnel to 2 Enterprise Branch Office LANs).

A VPN solution typically requires integration of several services (design, network management services, dial-up or dedicated access). Company that ensures coordination of services included in the solution is called *integrator*.

Enterprise Headquarters
Cisco® 1811 Router

```
sh run
Building configuration...
Current configuration : 8527 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ENTERPRISE
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$rP5K$... ... ...
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username cisco privilege 8
password 7 01100F175804
!
crypto isakmp policy 1
authentication pre-share
 group 2
crypto isakmp key NRjl... address 193.151.29.2
crypto isakmp key MJr3... address 193.151.30.2
crypto isakmp keepalive 10
!
crypto ipsec transform-set SET
esp-des esp-sha-hmac
!
crypto map BRANCH 10 ipsec-isakmp
 set peer 193.151.29.2
 set transform-set mirades
 match address 101
!
crypto map BRANCH 20 ipsec-isakmp
 set peer 193.151.30.2
 set transform-set mirades
 match address 102
!
interface FastEthernet0
 description LINK_to_L3
 ip address 193.151.31.2 255.255.255.248
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map BRANCH
!
interface FastEthernet1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 description LAN
 ip address 192.168.157.1  0.0.0.7
!
ip route 0.0.0.0 0.0.0.0 193.151.31.1
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.157.0
0.0.0.7 192.168.57.0 0.0.0.7
access-list 102 permit ip 192.168.157.0
0.0.0.7 192.168.57.8 0.0.0.7
!
control-plane
!
privilege exec level 8 traceroute
privilege exec level 8 ping
privilege exec level 8 show configuration
privilege exec level 8 show
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password 7 045802150C2E
 login local
 transport input telnet ssh
!
end
```

Enterprise Branch Office 1
Cisco® 831 Router

```
sh running-config
Building configuration...
Current configuration : 2132 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH_OFFICE_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$HdL9$... ... ...
!
no aaa new-model
!
dot11 syslog
!
ip cef
!
username cisco privilege 8
secret 5 $1$TdMn$LuvKyj7ZHW8rm8Pz7DIsm/
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp key GYz... address 193.151.31.2
crypto isakmp keepalive 10
!
crypto ipsec transform-set SET
esp-des esp-sha-hmac
!
crypto map BRANCH 10 ipsec-isakmp
 set peer 193.151.31.2
 set transform-set mirades
 match address 101
!
archive
 log config
  hidekeys
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
 description WAN
 ip address 193.151.29.2  255.255.255.248
 duplex auto
 speed auto
 crypto map BRANCH
!
interface Vlan1
 description LAN
 ip address 192.168.57.1 255.255.255.248
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 193.151.29.1
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.57.0 0.0.0.7
192.168.157.0  0.0.0.7
!
control-plane
!
privilege exec level 8 traceroute
privilege exec level 8 ping
privilege exec level 8 show crypto isakmp sa
privilege exec level 8 show crypto isakmp
privilege exec level 8 show crypto
privilege exec level 8 show configuration
privilege exec level 8 show
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login local
!
scheduler max-task-time 5000
end
```

Enterprise Branch Office 2
Cisco® 831 Router

```
sh running-config
Building configuration...
Current configuration : 2132 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH_OFFICE_2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$HdL9$... ... ...
!
no aaa new-model
!
dot11 syslog
!
ip cef
!
username cisco privilege 8
secret 5 $1$TdMn$LuvKyj7ZHW8rm8Pz7DIsm/
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp key KFj... address 193.151.31.2
crypto isakmp keepalive 10
!
crypto ipsec transform-set SET
esp-des esp-sha-hmac
!
crypto map BRANCH 10 ipsec-isakmp
 set peer 193.151.31.2
 set transform-set mirades
 match address 101
!
archive
 log config
  hidekeys
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
 description WAN
 ip address 193.151.30.2  255.255.255.248
 duplex auto
 speed auto
 crypto map BRANCH
!
interface Vlan1
 description LAN
 ip address 192.168.57.9 255.255.255.248
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 193.151.30.1
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.57.8 0.0.0.7
192.168.157.0  0.0.0.7
!
!control-plane
!
privilege exec level 8 traceroute
privilege exec level 8 ping
privilege exec level 8 show crypto isakmp sa
privilege exec level 8 show crypto isakmp
privilege exec level 8 show crypto
privilege exec level 8 show configuration
privilege exec level 8 show
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login local
!
scheduler max-task-time 5000
end
```

Fig. 4. VPN IPSec tunnel configuration between the enterprise headquarters and branch offices using Cisco® equipments.

Depending on the case, VPN solution integrator can be [12]:

- Customer himself (by the network administrator);
- One of equipment providers (e.g. equipments supplier can ensure the services integration against payment);
- An independent company, specializing in turnkey solutions.

In conclusion, as a general requirement for an infrastructure support is that enterprises must be able to interoperate and exchange information's and knowledge in real time so that they can work as a single integrated unit, although keeping their independence and autonomy. For the future, e-services, e-commerce and e-business require the enterprise re-thinking and re-modeling easy and fast the system and applications design for an efficient use of new network technologies.

The strategies develop and implement will require partnership and collaboration among the private, public and academic sectors as well as other agencies and organizations that strive to link them together. It will require the active involvement of consumers (clients, customers) and citizens (users of all kind).

Today, in the European countries, more than 95% of the companies are small and medium-sized enterprises and the majority of the European Union employees work in these companies. In this idea, the proposed collaboration infrastructure (based on VPN IPsec technology support), based on a virtual enterprise network, expect to reduce involvement of individual small and medium-sized enterprises in networking efforts, enable better and faster decision processes and promote the development of the business services sector. Because of the new product development paradigm, there is a greater need for software tools to implement a collaborative business system. Choosing partners for partnership creation is very important when seeking to increase the competitiveness of the enterprise in a virtual enterprise business network system and this represent a step in the process of virtual enterprise establishment. Companies are told that they will not survive in the modern Knowledge Society unless they have a strategy for managing and leveraging value from their intellectual assets, and many strategies have been proposed in the past years.

The software used for project management and for collaborative work should provide instant access to information and collaboration to support virtual team's members:

- to improve time management and knowledge management activities;
- to improve collaboration, co-operation and integration;
- to enhance revenue by responding swiftly and accurately by sharing products component information (costs, delivery date etc.) with stakeholders.

In fact, possible solutions to implement a VPN structures for a VEBN system realization in a geographically dispersed large enterprise or consortium are today:

- Local VPN based on VLAN (Virtual Local Area Network);
- Local VPN based on IPSec (Internet Protocol Security);
- VPN wide area based on IPSec;
- VPN wide area based on MPLS (Multiprotocol Label Switching);
- VPN based on PPPoL2TP (Point-to-Point Protocol over Layer 2 Tunnelling Protocol);
- UMTS (Universal Mobile Telecommunication System), etc.

The benefits services provided by VPN solutions in a VEBN are:

- the voice, video and data services convergence is done with low costs;
- Secure Remote Access to company resources;
- costs predictable and easier to budget, independent of traffic;
- the possibility of transferring any-to-any of data-voice-video applications;
- reliable support for LANs integration;
- security of data transmission;
- constant transfer rate, technological guaranteed;
- smart management solutions.

VPNs can be purchased from a telecommunications company and as an alternative they can create by using existing network infrastructure as the Internet or public switched telephone network, and software through the tunnel crossing.

In this context, IPsec solution purposed in the PREMINV e-platform [24] to create a VEBN (see Fig. 5), is a framework of open standards for ensuring private communications over public networks.

Also, it has become the most common network layer security control, typically used to create a virtual private network (VPN) for a VEBN application. IPSec Tunnel mode is used to secure gateway-to-gateway traffic. IPSec Tunnel mode is used when the final destination of the data packet is different from the security termination point. It protects the entire contents of the tunneled packets. The IPSec Tunnel mode data packets sent from the source device are accepted by the security gateway (a router or a server) and forwarded to the other end of the tunnel, where the original packets are extracted and then forwarded to their final destination device. IPSec tunnel

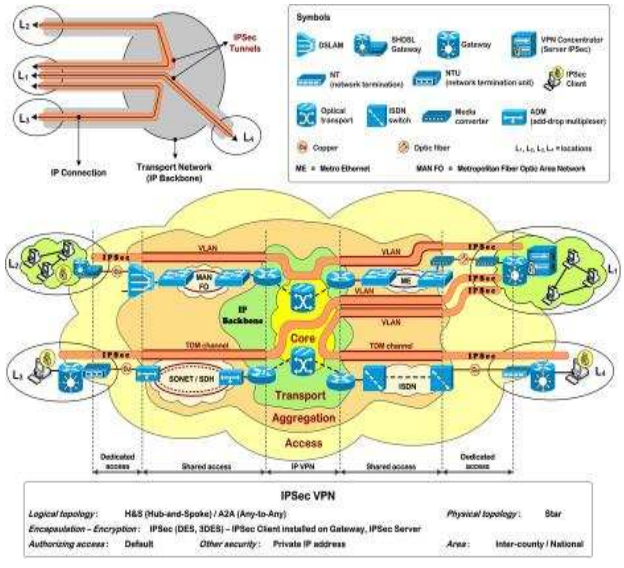

Fig. 5. Wide area based on VPN IPsec solution [24].

is usually built to connect two or more remote LANs via Internet so that hosts in different remote LANs are able to communicate with each other as if they are all in the same LAN.

4. CONCLUSIONS

In the actual context of the VEBN expanding, companies are much more preoccupied to build such structures and/or to be part of different structures that already exist. These will give them more business opportunities and by the knowledge transfer processes, they will gain competitiveness. Therefore, enterprises continue to implement information and communication technology systems solutions and strategies to improve their business processes in virtual networks. Clear trend is now evolving to intranets and extranets defined logic, which will lead to the reintegration of the various networks in single logical subdivisions with no physical. Structures that allow the approximation of this goal are virtual private networks.

Considering future product development as collaboration and communication oriented we implemented in the PREMINV platform a solution based on a virtual enterprise network (VPN IPSec) concept using integrated data sets and tools.

REFERENCES

[1] J. Niemann, S. Tickkiewitch, E. WestKamper, *Design and Sustainable Product Life Cycles*, Springer-Verlag, Berlin-Heidelberg, Germany, 2009.

[2] J.B. Ayers, *Handbook of supply chain management* (2nd Ed.), Taylor & Francis Group, New York, 2006.

[3] J. Kramer, J. Magee, *A rigorous architectural approach to adaptive software engineering*, Journal of Computer Science and Technology, Vol. 24, No. 2, 2009, pp. 183–188.

[4] T. Huang, G.Q. Wu, J. Wei. *Runtime monitoring composite Web services through tasteful aspect extension*. Journal of Computer Science and Technology, Vol. 24, No. 2, 2009, pp. 294-308.

[5] C.H. Hauser, D.E. Bakken, I. Dionysiou, H.K. Gjermundrod, V.S. Irava, J. Helkey, A. Bose, *Security, trust and QoS in next-generation control and communication for large power system*, Int. J. Critical Infrastructures, Vol. 4, No. 1/2, 2009, pp. 3–16.

[6] G. Dragoi, A. Draghici, S.M. Rosu, C.E. Cotet, *Virtual Product Development in University-Enterprise Partnership*, Information Resources Management Journal, Vol. 23, No. 3, 2010, pp. 43–59.

[7] L.J. Osterweil, *Formalism to support the definition of processes*, Journal of Computer Science and Technology, Vol. 24, No. 2, 2009, pp. 198–211.

[8] J. Husband, J. Bair, *Making Knowledge Work – The Arrival of Web 2.0*, Ark Group Press, London, 2008.

[9] J. Yu, A. Tappenden, J. Miller, M.A. Smith, *A scalable testing framework for location based services*, Journal of Computer Science and Technology, Vol. 24, No. 2, 2009, pp. 386–404.

[10] A. Shakya, H. Takeda, V. Wuwongse. *StYLiD, Social information sharing with free creation of structured linked data*, SWKM'2008, Workshop on Social Web and Knowledge Management @ WWW 2008, April, Beijing, China.

[11] M. Cudanov, O. Jasko, M. Jevtic, *Influence of Information and Communication Technologies on Decentralization of Organizational Structure*, Computer Science and Information System, Vol. 6, No. 1, 2009, pp. 93–109.

[12] S.M. Rosu, G. Dragoi, *VPN Solutions and Network Monitoring to Support Virtual Teams Work in Virtual Enterprises*, Computer Science and Information System, Vol. 8, No. 1, 2011, pp. 1–26.

[13] Cisco System, *Enterprise QoS Solution Reference Network Design Guide*, Cisco Systems, Inc., San Jose, CA, USA, 2008.

[14] R. Skoog, A. Von Lehmen, G. Clapp, J.W. Gannett, H. Kobrinski, V. Poudyal, *Metro network design methodologies that build a next-generation network infrastructure based on this generation's services and demands*, Journal of Lightwave Technology. Vol. 22, No. 11, 2004, pp. 2680–2692.

[15] H. Youssef, S.M. Sait, S.A. Khan, *Topology design of switched enterprise networks using a fuzzy simulated evolution algorithm*, Eng Appl Artif Intell, Vol. 15, 2002, pp. 327–340.

[16] S.M. Rosu, G. Dragoi, *Virtual Enterprise Network General Architecture, Proceedings of the 8th International Conference on Communications*, Bucharest, ©IEEE, 2010, pp. 313–316.

[17] S.M. Rosu, M.M. Popescu, C.A. Verisanu, *An Enterprise Network Management Solution*, Journal of Computer Science and Engineering, Vol. 2, No. 2, 2010, pp. 14–20.

[18] A.G. Mason, *Cisco Secure Virtual Private Networks*, Published by Pearson Education, Cisco Press, 2001.

[19] A. Moreno, K. Reddy, *Network virtualization*, Published by Pearson Education, Cisco Press, 2006.

[20] A.A.G. Walvoord, E.R. Redden, L.R. Elliott, M.D. Coovert, *Empowering followers in virtual teams: Guiding principles from theory and practice*, Computers in Human Behavior, Vol. 24, No. 5, 2008, pp. 1884–1906.

[21] J. Ward, J. Peppard, *Strategic planning for information systems*, West Sussex, England, John Wiley & Sons, 2002.

[22] G. Dragoi, C. Cotet, L. Rosu, S.M. Rosu, *Internet/Intranet/Extranet-Based Systems in the CESICED Platform for Virtual Product Development Environment*, Advances in Integrated Design and Manufacturing in Mechanical Engineering II, Tichkiewitch, S., Tollenaere, M., and Ray, P. (Eds.), Springer, XIV, 2007, pp. 293–307.

[23] R. Deal, *The Complete Cisco VPN Configuration Guide*, Published by Pearson Education, Cisco Press, 2005.

[24] S.M. Rosu, G. Drăgoi, *Virtual Enterprise Network Solutions and Monitoring as Support for Geographically Dispersed Business*, book chapter 3 in Handbook of Researchs on Business Social Networking: Organizational, Managerial, and Technological Dimensions, a book edited by M. Manuela Cruz-Cunha, Goran D. Putnik, Nuno Lopes, Patrícia Gonçalves & Eva Miranda, *(Eds)*, IGI Global 2011 pp. 34-62, DOI: 10.4018/978-1-61350-168-9.ch003, ISBN13: 9781613501689, ISBN10: 1613501684, EISBN13: 9781613501696, IGI-Global, 2011.