COMMUNICATIONS INTEGRATED NETWORK FOR EDUCATIONAL AND RESEARCH UNITS

Stefan-Victor NICOLAESCU[1)], Ioan LITA[2)], Ion BOGDAN[3)], Tudor PALADE[4)], Ion DUMITRASCU[5)]
[1)]Institutul Național de Studii și Cercetări pentru Comunicații, Bucharest
[2)]University of Pitesti,
[3)] Technical University Iasi,
[4)]Technical University Cluj-Napoca,
[5)]Institutul Naţional de Cercetare-Dezvoltare în Informatic, Bucharest
[1]stnicol@co.cnscc.ro, [2]ioan.lita@upit.ro, [3]bogdani@etti.tuiasi.ro, [4]palade@com.utcluj.ro, [5]dumitrascu@ici.ro

Keywords*:* multimedia, e-learning, virtual network, wireless

Abstract*: The paper deals with a project aimed to integrate activities between research institutes and universities. The aim of the project was to built up an integrated system research-education, in the communications domain. The paper presents the basis on which the integrated platform was achieved.*

1. INTRODUCTION

Integration and dissemination of educational and research activities means a wide spreading of knowledge between the partners engaged in research and education evolution. IT&C domain has a steady and quick development, and forecast studies indicate a sustained growth for the next years.

Consequently it is necessary a continuous change of information and documentations, conferences achievement, etc. between the IT&C research and development vanguard factors, firstly between researchers and universities peoples (professors, specialists, students, etc.), but also for graduated peoples and other specialists who want to obtain information about the most recent techniques and technologies of the domain.

The aim of the research (CERVIT project), developed in a partnership between two research institutes (INSCC, ICI) and three universities (University of Pitesti, UT „Gh. Asachi" Iasi, UT Cluj-Napoca) consists in building a complex infrastructure of a communication network for units spread over a large geographical area and an integrated set of methodologies, and associated services, tested and validated in collaborative activities (training, complex projects research, sharing of resources).

The network can be extended and new partners can participate to the network depending on their interest in the domain. Results can be adapted and expanded into other areas of education and research.

The project developed a trial, integrated network, IT-C, for educational and research units, in order to make possible various activities as:

- training courses and e-learning,
- communication (audio, video) between partners,
- libraries set up,
- experimental tests.

2. NETWORK TECHNOLOGY

IT-C virtual network structure for geographically dispersed education and research units, developed in the frame of the project is based on the principles of VPN (*Virtual Private Network*). VPN interconnects the private resources of two or many local networks through a public network. VPN is virtual because there is

no real connection between the communication points, and it is private, because the data transferred are available only for the partners associated.

VPN is a private connection between two or more networks or computers that send protected data by a public data network or by Internet. Thus, there are three typical scenarios for VPN solutions:

- An intranet spanning over several locations of a company;
- A dial-up access for home or field workers with changing IPs,
- An extranet for partners, which is the solution adopted for CERVIT Project. The solution needs different access to servers in the coordinator network than the partners.

VPN technology uses a combination of tunnels, encryption, authentication mechanisms and access control services, in order to carry traffic over Internet, over an IP network, etc.

VPN provides the possibility of communication using a public network infrastructure, with a good of data protection.

In other words, a virtual private network is a network of a company or a partners' association implemented on a common infrastructure, using the same security policies, management and performance, which usually applies to a private network.

Basically, virtual private network technology allows expanding the remote network services offered to users, representative or partner companies, via a public network, e.g. Internet.

VPN applications offer secure network to connections. A VPN tunnel must offer at least three important security services:

- authentication (for defining identities of terminal points of the tunnel);
- encryption (preventing the listening or intercepting of transmitted information through tunnel);
- integrity (to ensure that transmitted data are not changed during tunnel crossing).

The data packets are wrapped into one new package:

- Tunnel information (like the address of the other endpoint);
- Encryption data and methods;
- The original IP packet (or network frame).

and the new package is then sent to the other tunnel endpoint.

The solution for partners' communication networks must achieve at least the following vital functions:

⇨ User Authentication - The solution must verify the identity of the user and allow access through the VPN only to authorized users. In addition, the solution must allow for monitoring and record activities to show when and who accessed specific information.

⇨ Managing addresses. The solution must associate to the client a private network address and to ensure that private addresses remain secret.

⇨ Encryption of data. Data transferred via the public network must be made illegible to unauthorized customers.

VPN technology can be constructed on layer 2 [1] or on MPLS (*MultiProtocol Label Switching*) [2], [3], on SSL (*Secure Sockets Layer*) [4], etc.

Historically, VPNs were developed first over private leased telephonic lines and then over public networks [5]. Later the local networks were wireless configured, especially based on Wi-Fi equipments or a hybrid solution, wireless and wired were considered.

There are many different form to configure VPN. For example, SSL-VPN networks create a VPN over the public Internet, ensuring secure access to organization's resources for remote users as they would be located in the organization.

From the multiple possibilities of VPN configuration, two of them were considered thoroughly:

a. OpenVPN [6] is an open standard. It is a alternative of SSL-based VPN able of running over UDP (*User Datagram Protocol*). There are client and server implementations for all major operating systems.

b. "Hamachi" VPN Networks - "Hamachi" is a free, shareware application VPN without configuration (zero-configuration) able to establish direct links between PCs located behind some NAT (*Network Address Translation*) firewalls, without requiring reconfiguration (in most cases). Basically, it establishes a connection over the Internet

that emulates the links between computers in a local network.

Open VPN has two secure modes. The first is based on SSL/TLs (*Transport Layer*) security using public keys like RSA, and the second is based on using symmetric keys or pre-shared secrets. RSA certificates and the keys for the first mode can be generated by a specific command.

Although a VPN provides security and flexibility, it does not offer every time quality of service. In a VPN, end-to-end throughput is not guaranteed, and there can be packet losses, delivered out of order, and fragmented, depending of the transport network.

3. SOLUTION FOR PARTNERS MULTIMEDIA PLATFORM AND APPLICATIONS

The multimedia platforms designed and experimented [7], [8] as a test bed use modern information technologies for modeling of user and his experience, modeling of the user interface, designing of the human-computer interaction which assures a fast and steady exchange of information between network users as partners.

The subjects approached for training and information exchange refers to the most modern aspects of communication networks.

The multimedia communication platform developed in the frame of CERVIT Project consists of a local network at each partner (five local networks) and a central point located at Project's coordinator (INSCC), where is also located the administrator of the entire network. Partners' networks are based on advanced communication equipments, wired and wireless, able to offer different types of communications, both video and audio.

The partners' networks were individually developed and then interconnected by a transport network which offers a communication tunnel. The partners' access is secured by user name and password, assured by system's administrator. After entering the network of the project, the partners can add or modify documents, can start communication sessions in a secured manner (for example video or audioconference, etc.). Common data basis were created where the documents are available to all partners, except the case they are transferred in archive, from where can be recuperated if necessary, or can be deleted according to established rules. The platform can be in the future developed by integrating other education and research units.

By promoting the integrated network of educational-research, based on VPN structure, can be obtained the increase of the quality of education researchers, teachers, students and specialists in the IT & C, training young researchers from the ranks of students, expanding the network of education and research, ensuring the conditions for continuous education training etc.

In addition to data security, the partners are interested of the quality of services offered when trying to access certain applications remotely.

Acceptable levels for delays differ and are tolerated differently depending on the application.

Open VPN has a modular structure for networking and for security and uses stable mechanisms for authentication and for encryption, and communications connection can be easy tunneled, because VPN works very well with firewall. Excepting the effort needed to work with VPN, a weakness of the solution is that it is not IPsec compatible.

The network uses a security protocol through which the data are encrypted at source and decrypted only at destination.

Using VPN network technology, an educational and research integrated network, to provide broadband communications and to create the possibility of extending the coverage of various services, in locations with communication and education unfavoured infrastructure can be realized. To achieve the network modern wireless and cabled communication techniques were used.

VPN network specifications are based on the principle of maximum flexibility and swift completion. To achieve the VPN infrastructure for the CERVIT project was studied the main solutions and selected the most appropriate options, in line with project objectives and conditions. It was used a solution where the interconnection between partners networks is based on the public network, available to all partners.

In order to ensure secure VPN solution some principles must be fulfilled [9]. It is necessary to require a secure access control for VPN traffic, to limit management access, to add additional authentication (user name and passwords), to use dedicated devices for VPN termination (during VPN sessions), to limit configuration to specific users.

CERVIT virtual network development must be achieved by fulfilling requirements and maximum flexibility, scalability, fast performance, low cost. OpenVPN, which was chosen to ensure all those requirements, offers a simple alternative to other VPN technologies targeting small and medium-sized organizations and enables client and server implementations for all major operating systems.

The functional architecture of the virtual network it is a mesh type, because this type of architecture facilitates, at partner level, the communication "each with each" and even "each with oneself" (taking into account that in user level is intended to develop "platforms" that include multiple computers).

The users of the communication platform can gather themselves in a structure of closed „group users" by fully isolating their computers (perhaps temporarily) from the rest of the LAN.

The partners' local networks are mainly wireless, based on Wi-Fi equipments and are connected to Internet. Open VPN and Hamachi solutions were used to interconnect local networks.

In the realization of this architecture have been used terminal equipments as desktop computers, laptops, a pocket PCs and a wireless router.

The terminals were connected to the Internet through the router using wireless connections. Windows XP used by partners offer many VPN options that were not available in earlier versions of Windows, and the number of addresses is not limited by the Open VPN.

If the VPN only tunnels through the wireless link, the network will look exactly the same as it does without a VPN.

If the VPN extends beyond the wireless access points to pass through a wide area network such as the Internet, the wireless network client can appear to be part of a LAN in another building or far away, as it is the case.

The communication platforms were build VPN for all partners associated to the project and the connection between partners have been tested.

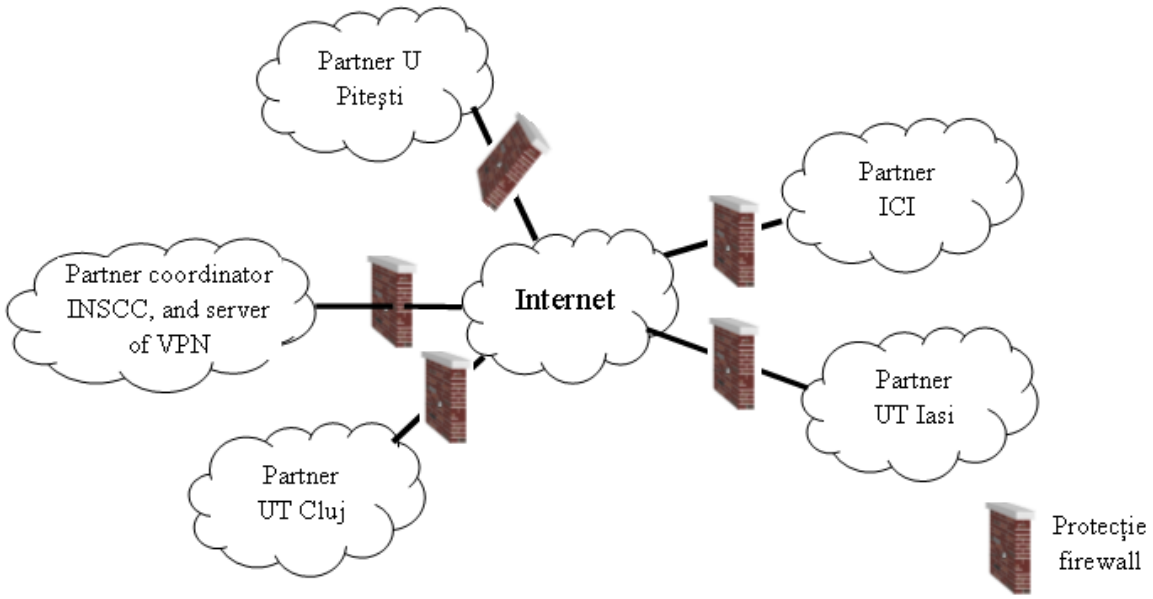

Fig. 1. The general structure of the VPN between partners.

The platforms of the university partners can be developed by extending them to the whole organizational structure (College, University, etc.).

The VPN server was installed at the coordinator of the project, which ensures its good functioning, development of access keys and passwords etc, and the partners LANs are interconnected by Internet.

The server was properly configured by the project's coordinator and it was uploaded with a new created database for training and e-learning in communication domain.

In order to upload data, the system's administrator attributed to each of the partners access keys and passwords.

Partners charged this database with documentation of training (courses, lectures, articles, etc.) for the communications.

Improving database and continue loading it with new documents will continue into the next stage so that eventually to constitute an active framework for exchanging information and experiences between universities and research institutes.

This type of "centralized" organization awarded to one of the partners (Project coordinator) the management of the entire virtual communication network.

This organizational model, justified by the heterogeneous experience in this domain of the participants in the project combined with large distances between them and possible difficulties in the communication, has advantages, but also involves taking in consideration some requirements.

The partners can obtain a limited remote control of the server, in order to do some experiments.

A firewall is a system that is the sole point of connectivity between the site it protects and the rest of the network. There should be no way to bypass the firewall via other gateways, wireless connections, or dial-up connections.

A firewall was installed to each of the partners and so a packet inspection is made (source IP address, source port, destination IP address, destination port, IP protocol and generally packet header information) [10].

Applications envisaged between project's partners include:

- Building up of virtual libraries;
- Multimedia conference;
- classes (series of specific thematic lectures) for graduated and students and young researchers;
- Experimental tests on the parameters of transmission quality and security of communications;
- Development of software for training and testing, etc..

In the common data basis the partners can add, modify or cancel documents, using the user name and password.

The old versions of documents or the cancelled ones are not really annulated, but they are collected in a folder which can be accessed only by network's administrator.

The system administrator is the only entity which can really erase the documents put into the spare folder.

That represents a protection and a basis for future eventually reconsideration of the documents. In order to communicate between them, partners can use audio or video communication.

The virtual network communication activity of CERVIT is supervised by two specific programs installed on the server:

- OpenVPN Access List Viewer,
- OpenVPN User Manager.

4. REFERENCES

[1]. Wei Luo: „*Layer 2 VPN Architecture*", Ed. Cisco Press, 2005
[2]. Ivan Pepelnjak, Jim Guichard: „*MPLS and VPN Architectures*", Ed. Cissco Press, 2002
[3]. Zhuo Frank Xu: „*Designing and Implementing IP/MPLS-Based Ethernet Layer 2 VPN Services"*, Ed. Wiley Publishing, Inc., 2010
[4]. Mark Lewis: „*Comparing, Designing, and Deploying VPNs*", Ed. Cisco Press, 2006
[5]. Barrie Sosinsky: „*Networking Bible*", Wiley Publishing, Inc., 2009
[6]. Markus Feilner: „*Open VPN – Building and Integrating Virtual Private Networks*", Ed. Packt Publishing, Birmingham, 2006

[7]. Ştefan-Victor Nicolaescu, coord.: „*Reţele wireless de acces – Alocarea dinamică şi autoorganizarea resurselor*", Ed. Printech, Bucureşti, 2010

[8]. Ştefan-Victor Nicolaescu, coord: „*Accesul wireless de bandă largă, vol 1 şi 2*", Ed Printech, Bucureşti, 2008

[9]. Anne Henmi, Mark Lucas, Abhishek Singh, Chris Cantrell: „*Firewall Policies and VPN Configurations*", Ed. Syngress Publishing, Inc. 2006

[10]. Jazib Frahim, Omar Santos: *CISCO ASA All-in-One Firewall, IPS, Anti-X and VPN Adaptive Security Appliance*, Second Edition, CISCO Press, 2010