American Research Journal of Humanities & Social Science (ARJHSS)
E-ISSN: 2378-702X
Volume-02, Issue-06, pp-64-68
June-2019
www.arjhss.com

Research Paper Open Access

Testing PKI and VPN infrastructure at the University of Culture, Sports and Tourism

Le Ngoc Hoan - Vu ThiThuy
Thanh Hoa University of Culture, Sports and Tourism, Vietnam
**Corresponding Author:* Le Ngoc Hoan

ABSTRACT:- *Public key infrastructure - PKI and a private network connection on a shared network (Virtual Private Network*-VPN) shows great efficiency in security and information security for organizations, enterprise. Therefore, they have been researched and developed by many scientists and organizations for current network systems and services. Researching and testing PKI infrastructure, a virtual private network (VPN) applies to Universities ThanhHoa Culture, Sports and Tourism. The research focuses on research on PKI infrastructure and VPN on the basis of theory. After that, building on the testing environment is to build and connect on LAN system at 2 campuses of the school on windows server 2012.

Keywords: Public key, PKI infrastructure, Virtual private network, Security, Safety and security.

I. INTRODUCTION

The development of security policies and mechanisms, security for systems and transmission lines is quite diverse and popular. In particular, the application of PKI infrastructure for the most common security and security issues is bringinggreat efficiency. Understanding and building PKI infrastructure in conjunction with VPN infrastructure are an approach for a new platform that we can deploy to test and apply to practice to improve managing efficiency in order to meet the needs of data access and applications for remote users via the internet. The research results can be applied to all branch offices, between offices need to exchange data with each other.

II. IMPLEMENTATION REQUIREMENTS

***Connection**

Designing requirements set out to build a secure connection system among facilities, units are far from the Center on the basis of making the most of available equipment and network infrastructure of the University of Culture, ThanhHoa Sports and Tourism. This system is compatible with current applications, flexible, compatible with various connection infrastructure such as ADSL, LeaseLine,.

***Security**

To ensure a safe connection to the main building (establishment 1), it requires a solution:
- Using modern security technologies.
- Flexibly change security methods.
- Supplementing security methods to ensure safety and security.

***Administration**

Ensuring the continued operation of the network, the solution must design the monitoring software; administer the VPN Server system at the main facility. The software has the ability to monitor connections. Network administrators must fully and regularly capture information about configuration, problems and all data related to network usage.

***Reasonable investment costs**

In order to make the solution feasible, in addition to technical requirements, security ... the investment cost is one of the most important requirements. When deployed with the model and the number of branches connected to large start-up costs are huge. With the introduction of a reasonable investment solution, it will create favorable conditions for application in practice.

III. RESEARCH METHODS

3.1. Selection model

The test model is a remote virtual private network model using common software and available products currently that are being exploited on the network of the ThanhHoa University of Culture, Sports and Tourism.

Remote access clients are personal computers with modems, the operating system of Windows XP or Windows 7, Windows 10, etc. The machine is configured as a VPN client.

A server is a central machine installed with Windows server 2012. The server has 2 network interfaces, with routing and remote access services. In these two interfaces, an interface is used to connect to the internet via ethernet. The other interface is used to connect to the local network via ethernet with the IP address configured as a VPN server.

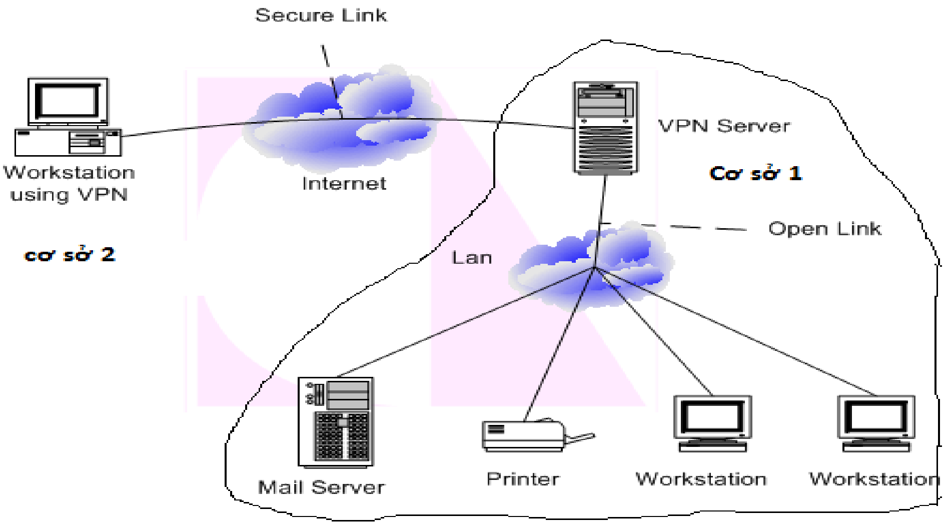

Figure 3.1. Remote access network model

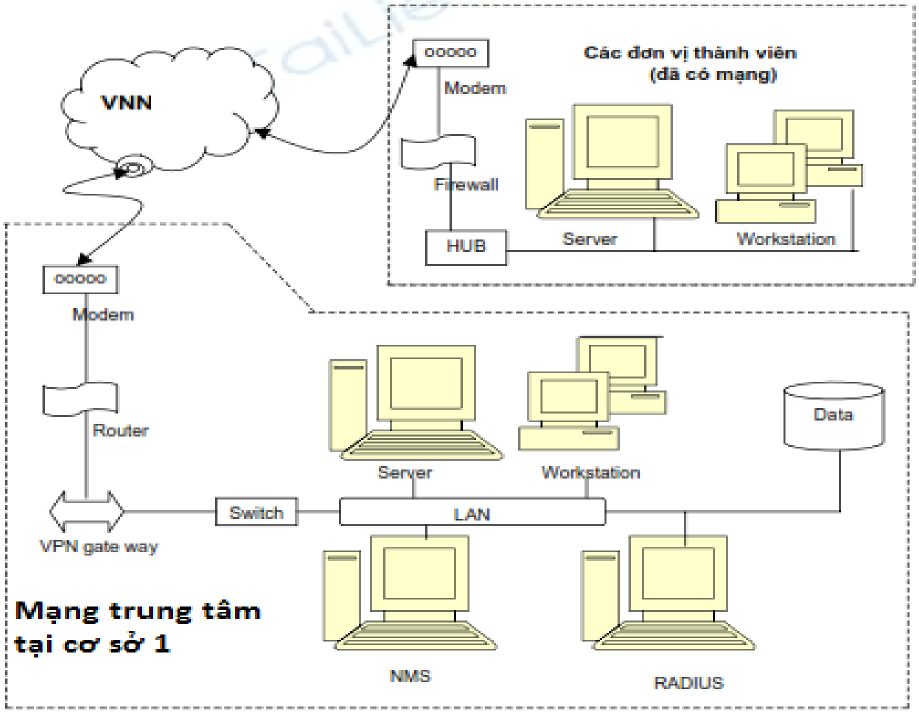

Figure 3.2. Building network system at school to test PKI, virtual private network for ThanhHoa University of Culture, Sports and Tourism

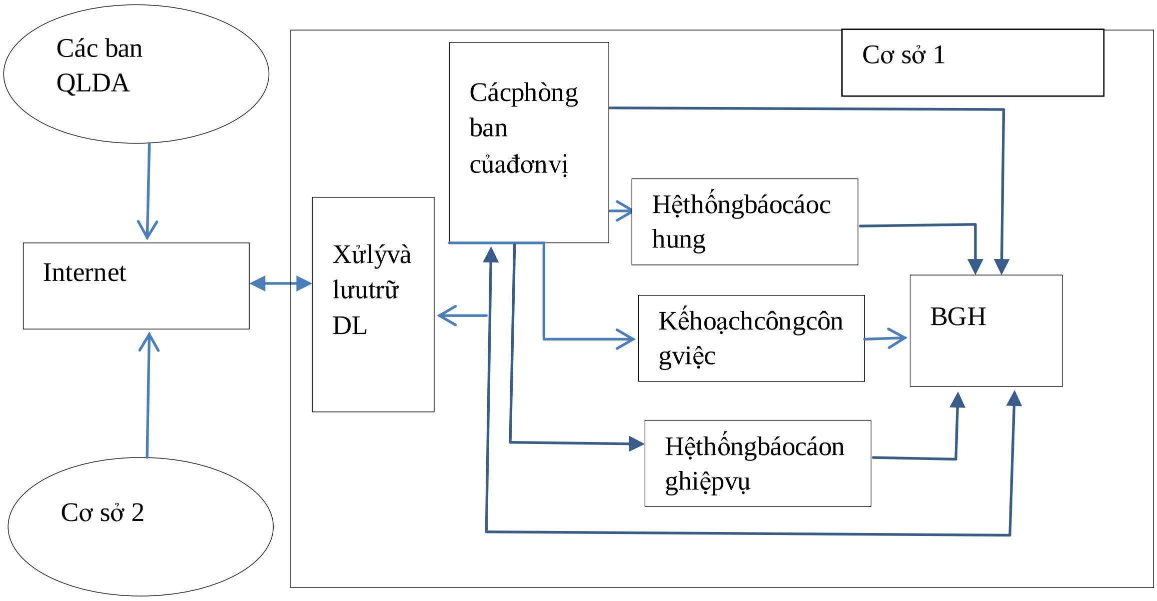

Figure 3.3. Data flow diagram

3.2. Selecting tools, implementing installation

- Using the operating system of Windows server 2012 installed on the Server machine;
- Client machines using the operating systems of Windows XP, Windows 7 or Windows 10;
- Routing routers;
- Other necessary connection devices
- Connection settings in the system:

1. Computer Server installed windows server 2012is setup PKI and VPN infrastructure, with 2 network interfaces.
2. Client machines in LAN network connect directly with a server that is located at the establishment 1.
3. Client machines outside the system are located at the establishment 2 connecting computers in the system at the establishment 1 by separate pipelines via the server with a separate policy.

- Specific deployment:

B1. Installing windows server enterprise 2012 on the server (the VPN server)
B2. Installing Internal Client machines in the LAN network at the establishment 1 with the server.
B3. Installing the External Client at the establishment 2 outside the LAN system - Set up a connection for Client and Server
B4. Setting up Network Adapter for Internal Client; Setting up the IP address for connections in the system.
B5. Setting up Network Adapter for External Client
B6. Setting up Network Adapter for Server
B7. Setting up VPN for users with their own policies
B8. Setting up a VPN for the user (Client)
B9. Setting up a policy for the user - Network policy and Access service
B10. Setting up the Routing and Remote Access Service for the Client
B11. Checking information the 1 Client connected to the system via the VPN created by the server
B12. Setting up Remote Access for external clients
B13. Testing client outside connecting data access to Client in the LAN system via VPN

4. Evaluating the effectiveness of research and system test deployment

4.1. These achievements

For the purpose of the project "Testing PKI infrastructure, a virtual private network for the ThanhHoa University of Culture, Sports and Tourism". I have conducted research and presented research results on issues:

***About infrastructure:**

- Material facilities for information technology are met to be able to deploy and build systems such as computers, transmission lines, and connected devices.
- Having sufficient force of technicians and lecturers to ensure knowledge to participate in deploying and operating the system.
- ADSL high-speed internet service uses a fiber optic transmission line, ensuring good transmission speed.

- Units: departments, faculties, and centers are fully equipped with computer systems, ensuring common configuration.

***About models and options**

On the basis of application requirements set out: building applications of PKI infrastructure and virtual private network applied to the ThanhHoa University of Culture, Sports and Tourism. The first step is to identify the model of PKI architecturewith only one CA, which is applicable only to faculty members at centers, departments, and faculties of two campuses with a small number of visits. Therefore, the model is built with the following criteria and requirements:

- The construction model is not too complicated and responsive to remote access, ensuring convenience and ensuring information security during exploitation and exchange, in accordance with general conditions and requirements in management and exchange of school information.
- A model is a form of ensuring the convenience, quickness, security and information security for small and medium-sized units and organizations with the use of PKI infrastructure and virtual private network to reduce the cost; proactive in managing and operating information compared to using services of suppliers in the market.
- The model can be developed and expanded when the system increases the need to use and scale the system or has plans to cooperate with units outside the school system.

*** Implementation policies and services for information security**

✓ **IP address management**

The boom in the use of IP to transmit data, both inside and outside the network of companies, businesses, etc. leads to some problems in IP allocation and management. Initially, the IP address space is 32 bits (IPv4). However,

The issue of dynamic IP has solved the allocation of IP addresses and routing, but it has complicated the construction of the VPN. IPSec is a protocol, which may be the most suitable for use with IPv6, but most of them must be compatible with IPv4 and have more mechanisms to solve problems. One solution to increase the IP address management space is the use of IP in a virtual private network (VPN) that remains connected to the public internet.

✓ **Building PKI security**

Currently, many virtual private networks (VPNs) are showing limitations because the security system itself is too simple. The problem is to be able to meet the requirements of developing a large and highly secure virtual private network. Most virtual private networks today are being exploited without the use of public key infrastructure (PKI). In the simplest way, it can be done by setting up the configuration at both ends of the VPN tunnel and sharing a common secret - a pair of passwords.

Two VPN terminals can be authenticated through an electronic certificate - A kind of "electronic membership card" that is indispensable in large VPN networks. For electronic certificates, this organization is called a certification system (CA-Certification Authority). VPN networks use electronic certificates when the IP tunnel is initialized, the endpoints will authenticate each other through electronic certificates. Public key infrastructure will play an important role in successfully building large VPN networks.

✓ **Building a firewall**

A firewall is a solid barrier between a private network and the Internet. We can set up firewalls to limit the number of open ports, packet types, and protocols that are passed.

The firewall will partition policy areas and set access policies for remote access to the system. This solution ensures control and policy settings for the VPN address space.

✓ **Management solution**

Management solution is indispensable for managing VPN network with a large number of connections. Administration and configuration work through the command line. This makes it difficult to monitor the connection to the system, make configuration for newcomers to access the system.

✓ **Quality of service management**

To coordinate various forces in the multi-service network, including the transmission of messages, online transactions, multimedia data,…createmany difficulties for bandwidth allocation and network management.

Network traffic and VPNs are inextricably linked to addressing congested traffic and bandwidth, including:

- Providing excess network bandwidth
- Securing the bandwidth
- Prioritizing traffic (service delivery)
- Providing static resource.

4.2. Proposals and directions for development

With PKI infrastructure, deploying a single CA always meets the operational needs of an enterprise or a medium-sized unit, ensuring flexibility and ease of deployment. However, with the requirement that when a virtual private network system is scaled up for many users and linked to units outside the LAN system, a CA is difficult to secure and manage safely. So it can be upgraded to a decentralized CA model with a CA as the central control, each of which is a child CA.

Roaming issues between ISPs and the ability to combine MPLS with IPSec to extend VPN boundaries and enhance VPN security.

The ability to apply IPv6 to VPN services and the ability to deploy internet infrastructure will increase the ability to manage and distribute IPs in VPNs.

REFERENCES

[1]. Bàigiảng An toànvàBảomậtthông tin PGS.TS.NguyễnKhanhVăn, ĐạihọcBáchKhoaHàNội, khóacaohọcCôngnghệthông tin 2012,.

[2]. Brian Komar, Windows Server 2008 PKI and Certificate Security, Microsoft Press, 2008.

[3]. Building and Managing Virtual Private Networks, Dave Kosiur, Wiley & Sons; ISBN: 0471295264.

[4]. Cryptography and Network Security Principles and Practices_ 4th Ed - William Stallings, Copyright 2006.

[5]. Mạngriêngảo: côngnghệvàtriểnkhaiứngdụng, Luậnvănthạcsỹ, NguyễnThạcThanhQuang, 2004.

[6]. Network Security Technologies, Second Edition, Kwok T. Fung, Auerbach publications, 2005.

[7]. Virtual Private Networking Basics – Conputer, By NETGEAR, Inc. All rights reserved, v1.0, October 2005.

Corresponding Author: Le Ngoc Hoan
Thanh Hoa University of Culture, Sports and Tourism, Vietnam