Fall 10-2012

Implementing Virtual Privat Network in Small to Medium Sized Enterprises

Fatos Xhemajli

Faculty of Computer Sciences and Engineering

Implementing Virtual Privat Network in Small to Medium Sized Enterprises

Bachelor Thesis

Fatos XHEMAJLI

October / 2012

Prishtinë

Faculty of Computer Sciences and Engineering

Bachelor Thesis

Academic Year 2001 - 2012

Student: Fatos XHEMAJLI

Implementing Virtual Privat Network in Small to Medium Sized Enterprises

Supervisor: Petrit SHALA

Date: October/2012
Prishtinë

This thesis is submitted in partial fulfillment of the requirements for a Bachelor Degree

ABSTRACT

Nowadays enterprises rely heavily on computer systems for storing and processing vital information, IT plays a major role in their businesses therefore all these systems must be safe and reliable. Computer networks are a major part of all these technologies; they provide the essential link between them, connecting them into one unified information network. However, the main requirement in all this is to implement a proper security system that will keep all these information secure and protect the privacy.

Small or medium-sized enterprises need to have their branches interconnected with a rapid, reliable, cost-effective access to their resources.

The ability to reach important company resources enables the employees to be more flexible and productive, especially when they have the flexibility to access those resources from remote offices, home, or when traveling. This level of connectivity is a core component of IT strategy in today’s business world and is critical for staying ahead of the competition.

Virtual Private Networks (VPN), present businesses a solution to this need. A VPN allows an enterprise to build a secure communication network by leveraging the public Internet as a low-cost transportation mechanism. This increasing use of VPN is one of the key growth drivers for the increased deployment of firewalls.

CONTENT

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The setup of a good network infrastructure is not difficult when the enterprise has only one office. The difficulty starts when requests are to communicate with other branches/offices in different countries or cities. The employees of one branch/office want to use the networks of other sites without encountering problems.

To achieve this, the exchange of data or the access to several files has to be the same on all networks. We want to create one big network for the whole enterprise. To accomplish a good and secure connection between several branches/offices, we will use a VPN network (Virtual Private Network).

There are two very important parameters to take care of when designing such networks; Security and Confidentiality.

In the past, organizations or enterprises would physically install lines over large distances to ensure secure data transfer. However, this system is impractical for every enterprise and everyday users due to the cost, space, and time required for such installations. The concept of Virtual Private Network (VPN) is not new – technologies such as Frame Relay (FR) or Asynchronies Transfer Mode (ATM) have been used over the last decades as a basis for the implementation of this concept. Whatever the format or the technology behind it, a VPN provides a service functionally equivalent to a private network using resources of a public network.

In recent years, with the exponential growth of the Internet, the landscape of telecommunications has changed radically and the Internet has become part of almost every aspect of the developed world including education, banking, business, and politics. Over the past two decades the Internet has been found to be vulnerable to attackers seeking sensitive information. The most recent solution to this problem has been IP-based Virtual Private Network (IPVPN) [1].

1.1 Background

Virtual Private Network (VPN) can be defined as a network which provides secure communication among multiple sites through use of public telecommunication infrastructure with the same access or security policies as a private network through the use of tunneling protocols. VPN systems provide users with the illusion of a completely private network [2]

The fundamental benefit of a VPN is the ability to quickly, easily, and cost-effectively set up a secure high-speed wide-area or remote-access connection. You can use VPNs with many different high-speed options including ISDN, DSL, cable, and wireless.

This flexibility allows you to take advantage of the best and most cost-effective options available. A VPN can be built on the Internet or on a service provider's infrastructure.

There are two types of VPNs—remote access and site-to-site.

With remote-access VPNs, remote workers enjoy secure, encrypted, high-speed access to the company's network resources just as if they were in the office. Remote-access VPNs enable you to make more effective use of mobile and remote workers while saving on the costs of office space and phone charges.

Site-to-site VPNs are used to connect remote offices to each other and to headquarters, or to connect your company to another company, such as a customer, supplier, or partner.

1.2 Problem Statement

A microfinance institution in Kosovo, which started its operation recently in the capital Prishtina and has been successful in providing its services, is interested to make a step in the improvement of the provision of its services. They are interested to open their branches in the entire territory of the Republic of Kosovo in order to cover all the territory with their services, this will be supported by a centralized infrastructure (head office) that provides HR, IT and supply chain management support.

One of the challenges in the achievement of this purpose is the exchange of important information between the central office and local brunches safely and confidentially, by using public infrastructure which shall reflect more cost effective.

1.3 Thesis Outline

This thesis consists of 7 chapters. Chapter 1 describes the background of the thesis. Chapter 2 explains the VPN basics and gives a general overview. Chapter 3 describes in detail the VPN Tunneling types and methods. In Chapter 4 are explained the cryptography concepts and methods. Chapter 5 gives the proposed solution for implementing VPN. Chapter 6: thesis summary. References are given in Chapter 7, VPN configuration script is given as annex in Chapter 8.

2. VIRTUAL PRIVATE NETWORK (VPN)

2.1 Overview

Before the creation of VPN technologies, the only way for companies to secure network communications between different locations was to purchase costly dedicated connections.

VPNs allow companies to create secure encrypted tunnels between locations over a shared network infrastructure such as the Internet. A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure. IETF gives the next definition: "VPN is defined as the emulation of a private WAN through public networks". [2]

VPNs are broken into three types based on their usage:

- **Access VPNs** — An access VPN, shown in Figure (1), provides secure communications with remote users. Access VPNs are used by users who connect via dialup or other mobile connections. A user working from home would most likely use an access VPN to connect to work. Access VPNs usually require some type of client software running on the user's computer. This type of VPN is commonly called a remote-access VPN.

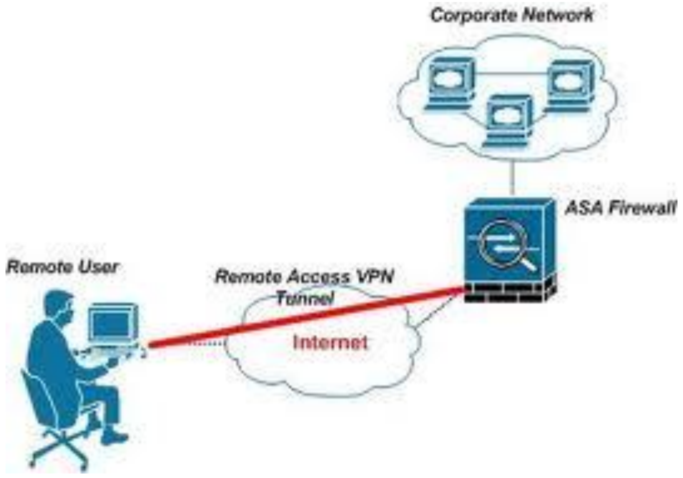

Figure 1: Access VPN [22]

- **Intranet VPNs** — An intranet VPN is used to securely interconnect a company's different locations. This allows all locations to have access to the resources available on the enterprise network. Intranet VPNs link headquarters, offices, and branch offices over a shared infrastructure using connections that are always encrypted. This type of VPN is normally configured as a site-to-site VPN.
- **Extranet VPNs** — Extranet VPNs provide a secure tunnel between customers, suppliers, and partners over a shared infrastructure using connections that are always encrypted. This type of VPN is also normally configured as a site-to-site VPN. The difference between an intranet VPN and an extranet VPN is the

network access that is granted at either end of the VPN. Figure (2) shows a site-to-site VPN, the configuration commonly used for both intranet and extranet VPNs.

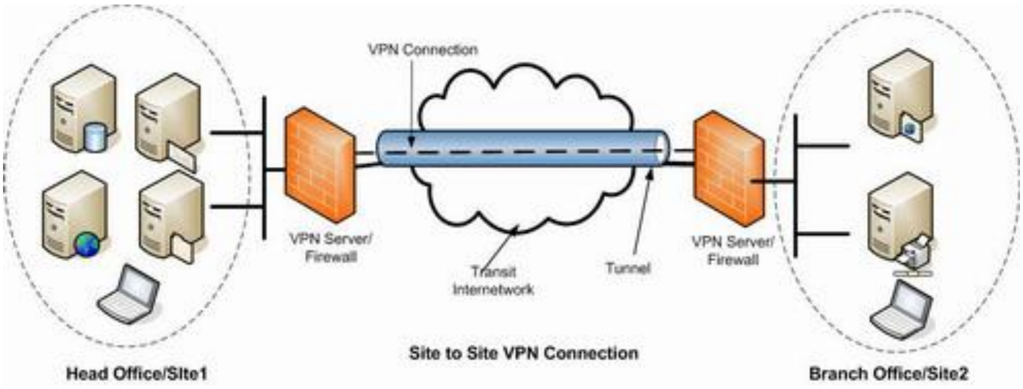

Figure 2: Site-to-Site VPN [23]

2.2 What is VPN?

A virtual private network (VPN) is an extension of a company’s private intranet across a public network such as the Internet. It creates a secure private connection through a private tunnel. VPNs securely connect remote users and offices in a corporate network. The objective of a Virtual Private Network is to add a level of security to the exchange of data. Even when a company is using a leased line, they can deploy a VPN network to protect their data. [3]

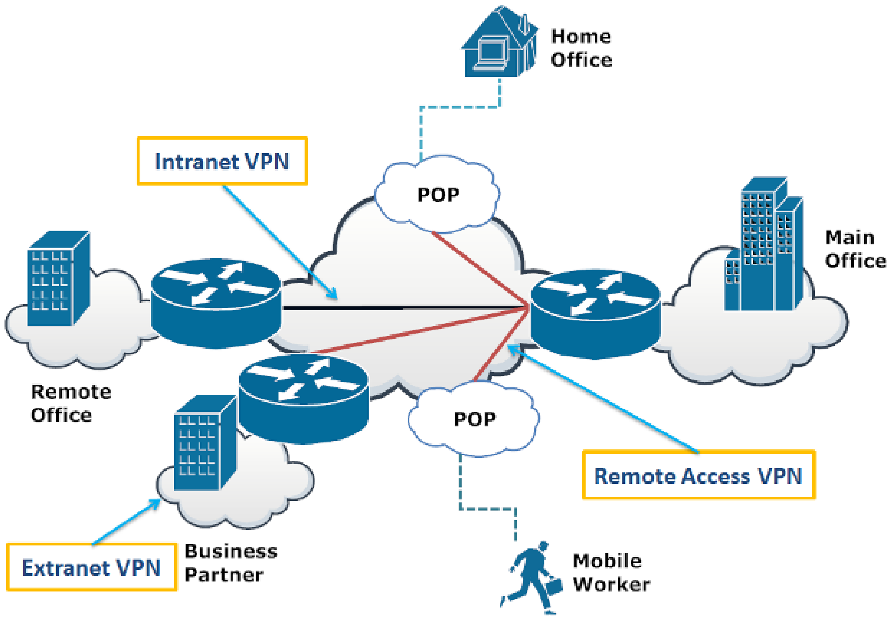

Figure 3: VPN Topology [24]

2.2.1 Concepts used by a VPN

To achieve the objective of a VPN, we have to make use of some extra technologies and mechanisms. The initial concept of the Internet is not designed for this kind of utilization.

2.2.1.1 Tunneling

The exchange of data in a corporate intranet is rarely routable along the Internet. Either the enterprise uses a protocol that differs from the standard Internet protocol (IP) or the internal network address pool is only valid on the intranet. (We call these private addresses). By using tunneling protocols, we can encapsulate a non-routable packet into a routable packet and send the data to our receiver along the Internet. By adding some encryption and signature mechanisms we can provide a secure data exchange. Examples of tunnel protocols are GRE, L2TP, PPTP and recently SSL.[4]

2.2.1.2 Authentication

The Internet is a widely used network with millions of computers and servers connected. All these entities can connect to the resources of the company. Thus it is highly necessary, when implementing a VPN, to assure the identity of all the users that connect to the company’s resources via the VPN. We can obtain this by using proper authentication methods.

2.2.1.3 Encryption and signatures

All VPNs rely on the use of a public and most of the time shared network. The confidentiality and integrity of the exchanged data are not assured by this public infrastructure.

Virtual private networks make use of several encryption techniques and digital signatures to assure that only the right person can use the exchanged data (confidentiality) and that the data is not changed or modified during transport (integrity).

2.2.2 Common VPN scenarios

We can use VPNs in several different contexts. I will explain the three most common scenarios.
• Site-to-site VPN
• Client-to-site VPN
• Extranet VPN

2.2.2.1 Site-to-site connection

A Site-to-site connection is used to link branch offices with the company's headquarters. This scenario securely interconnects trusted intranets within an organization. The security focus is both, protecting the company's intranet against external intruders and securing the company's data while it flows over the public Internet. It can totally replace leased lines or PVC networks. It will be less expensive, more secure, and globally accessible. One way to implement this VPN connection between the corporate offices is to purchase Internet access from an ISP (Internet Service Provider). Firewalls and VPN servers can be placed at the boundary of each of the intranets to protect the company's traffic from intruders. With this scenario, the clients and servers do not need to support VPN technology, since the VPN capabilities, data authentication and encryption, are provided by the VPN servers. With this approach, any confidential information would be hidden from untrusted Internet users, with a firewall denying access to attackers. [4]

With this scenario, the company's offices will be able to communicate securely with each other, whether local or far away. Through VPN technology, each branch office can also extend its existing intranet to incorporate the other branch intranets, building an enterprise-wide corporate network.

2.2.2.2 Client-to-site VPN

A remote user (or roadwarrior), whether at home or on the road, wants to be able to communicate securely back to the corporate intranet. For example, an employee is at home or on the road but needs a file on a server within the intranet. By obtaining Internet access the employee can communicate with the server in the company's intranet and access the required file.[4]

One way to realize this scenario is to use a remote access tunneling protocol. Another way is to use a VPN-enabled remote client and a VPN-enabled firewall; ideally, you can combine both solutions, which will provide the best protection. The client accesses the Internet via dial-up or a broadband connection to an ISP, and then establishes an authenticated and encrypted tunnel between him and the firewall at the intranet boundary. By applying authentication between the remote client and the firewall, you can protect your intranet from unwanted IP packets. And by encrypting traffic that flows between the remote host and the firewall, you can prevent outsiders from sniffing the exchanged information.

2.2.2.3 Extranet VPN scenario

A company wants their business partners to be able to access several resources on the corporate intranet. Because the company cannot control the business partners' networks, the company has to build a secure gateway to provide the necessary information. By using a VPN the company can provide this in a safe and secure way. A VPN can be built between a client in a business partner's intranet and the server in the company's intranet. The clients can authenticate themselves to the firewall, directly to the server, or to both. Then a tunnel can be established to encrypt all data from the client, through the Internet, to the server.[4]

The big difference between an Extranet VPN and a site-to-site scenario is the fact that the business partner's intranet is not a trusted network so an extra security level has to be added.

2.2.3 Advantages and inconveniences

To compare the solutions, to interconnect branch offices with a headquarters, we can distinguish several parameters.

- Costs
- Implementation time
- Performance
- Security

2.2.3.1 Costs

To set up a VPN network, you need only a proper Internet connection, when possible a high bandwidth connection. The cost of a connection nowadays is affordable for any company. The only extra costs are the extra hardware needed to set up your VPN. This is a big advantage over other solutions like leased lines or PVC/SVC's. For these you have to count in the extra subscription costs that need to be payed to the service carriers. The extra costs are negligible in a VPN setup, when you want to add extra sites or roadwarriors.

2.2.3.2 Implementation time

The biggest advantage of a VPN is the fact that it does not depend on a physical infrastructure. When there is an Internet connection present, it takes some weeks to implement everything in a big enterprise environment. Even if you want to add an extra site to an existing VPN it takes only a couple of hours to implement.

The implementation of a PVC/SVC is much more complicated because you have to rely on your service carrier who has to implement the extra lines and routes. Leased lines can take some months or even a year, depending on the service provider.

2.2.3.3 Performance

In this area, the VPN approach is not the best solution. Because a VPN makes use of a public infrastructure, parameters such as bandwidth, response time and QoS (Quality of service) are difficult to master by the network administrator. The performance of a VPN between two sites depends on the performance of the Internet between these two sites. But nowadays, the ISP networks have developed enough to provide a convenient service on which to implement a VPN. Leased lines or PVC/SVC networks do not suffer these public performance problems. The service carrier guarantees a good performance by using special techniques which are impossible on a public Internet. [1]

2.2.3.4 Security

A VPN relies on encryption methods which are very solid and secure. The generations of the encryption keys are handled by the owner of the VPN network. Due to this a VPN guarantees the exchanged data a high level of security. Leased lines are considered as the most secure network connections because it is a private line only used by the company. But the offered level of security depends on the company’s confidence in the service carrier. The service provider can eavesdrop on all the data that flows over the company’s network. One solution is to implement the leased lines oneself but being quite impossible, unlikely to result. Another solution is to encrypt all the exchanged data, which brings us back to a VPN network.

A VPN is the most vulnerable way to implement a WAN network, because of the public infrastructure used. Because of these problems, integrity and encryption are extensively employed to protect all the data. [1]

3. VPN TUNNELING PROTOCOLS

For a tunnel to be established, both the tunnel client and the tunnel server must be using the same tunneling protocol. Tunneling technology can be based on either Layer 2, Layer 3, Layer 5, or label switching tunneling protocol which are corresponding to the Open Systems Interconnection (OSI) Reference Model [4].

3.1 LAYER 2 Tunneling Protocols

These correspond to the Data-Link Layer and uses frames as their unit of exchange. Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) both operate at this layer and both encapsulate the payload in a Point to Point Protocol (PPP) frame to be sent across an internetwork.

3.1.1 Point to Point Protocol (PPP)

Because PPTP and L2TP depend heavily on the features originally specified for PPP, it is worth examining this protocol more closely. PPP was designed to send data across dial-up or dedicated point-to-point connections. For IP, PPP encapsulates IP packets within PPP frames, and then transmits the PPP-encapsulated packets across a point-to-point link. PPP was originally defined as the protocol to establish a connection between a remote client and an enterprise network through a Remote Access Server (RAS) as shown in Figure (4) [5].

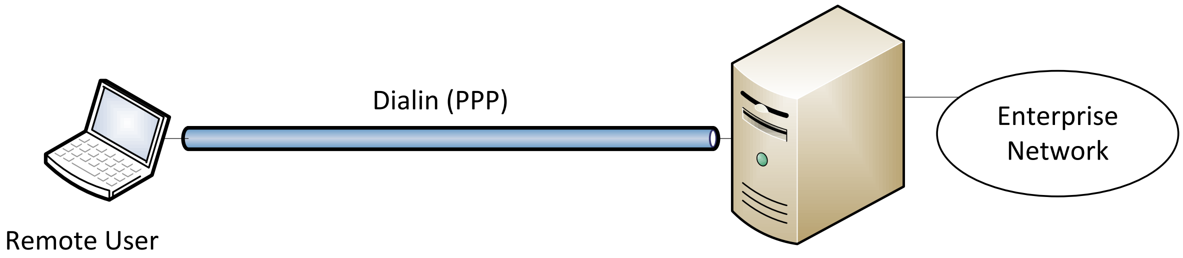

Figure 4: PPP Architecture [5]

Each PPP frame contains the following fields [5]:

- Flag field indicates beginning or end of frame. This field consists of 0x7e
- Address field carries the station ID in multidrop lines. Because PPP is point to point protocol, this field is not necessary and is set to 0xff.
- Control field specifies the type of data in the information field and is always set to
- 0x03
  Protocol field identifies the encapsulated protocol in information field.
- Information field contains the datagram for the protocol specified in the protocol field.
- Frame check Sequence (FCS) field is a standard 16-bit used for error detection.

There are three distinct phases of negotiation in a PPP connection. Each of these three phases must complete successfully before the PPP connection is ready to transfer user data.

- Link Control Protocol (LCP)
- Authentication
- Network Control Protocol (NCP)

3.1.2 Point to Point Tunneling Protocol (PPTP)

PPTP is a standard tunneling protocol developed by PPTP Forum which consists of Microsoft and some remote access vendors. Basically, PPTP is an extension of PPP, which encapsulates PPP frames in IP datagrams for transmission over an IP-based network, such as the Internet or over a private intranet. Figure (5) shows that PPTP architecture divides the RAS functions between a PPTP Access Concentrator (PAC) and PPTP Network Server (PNS). The remote clients dial into PAC, and PNS terminates remote clients' PPP session, provides access to the enterprise network, and acts as server for one or more PACs [6].

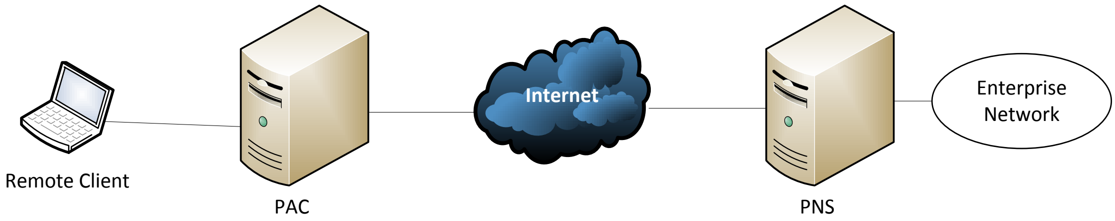

Figure 5: PPTP Architecture [6]

PPTP uses a TCP connection (restricting its use to IP networks), known as the PPTP control connection, to create, maintain, and terminate the tunnel. PPTP uses a modified version of Generic Routing Encapsulation (GRE) [7] to encapsulate PPP frames as tunneled data, which gives PPTP the flexibility of handling protocols other than IP, such as Internet Packet Exchange (IPX) and Network Basic input/output system Extended User Interface (NetBEUI). The payloads of the encapsulated PPP frames can be encrypted, compressed or both. Tunnel Maintenance with the PPTP Control Connection There is a PPTP control connection between the PPTP client and the PPTP server using the reserved TCP port 1723. The PPTP control connection carries the PPTP call control and management messages that are used to maintain the PPTP tunnel. This includes the transmission of periodic PPTP Echo-Request and PPTP Echo-Reply messages to detect a connectivity failure between the PPTP client and PPTP server. PPTP control connection packets consist of an IP header, a TCP header, a PPTP control message, and a data-link trailer and header as shown in Table (1).

Data link header	IP header	TCP header	PPTP control message	Data link trailer

Table 1: PPTP Control Connection Packet [7]

PPTP Data Tunneling

Table (2) shows the PPTP data tunneling steps. The initial PPP payload is encrypted and encapsulated with a PPP header to create a PPP frame. The PPP frame is then encapsulated with a GRE header. The resulting frame is then encapsulated with an IP header containing the source and destination IP addresses for the PPTP client and PPTP server. [6]

Data link header	IP header	GRE header	PPP header	PPP payload (IP datagram)	Data link trailer

Table 2: PPTP Data Tunneling [6]

PPTP-based VPN

The PPTP control massages deals with encryption or authentication. That’s because PPTP really is a tunneling protocol, not a VPN protocol.

PPTP relies on the underlying PPP for its encryption and authentication services. PPTP has a relatively low overhead which makes it faster than some other VPN methods. Even though PPTP supports site-to-site VPNs, it is best suited for remote access VPNs.

Microsoft has included PPTP clients in all versions of Windows since Windows 95 and PPTP servers in all its server products since Windows NT 4.0. PPTP has been very popular, especially on Windows systems, because it is widely available, free and easy to set up. The encryption is provided by Microsoft Point to Point Encryption (MPPE), which uses RC4 symmetric stream cipher algorithm, and the authentication is provided by Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), which is the Microsoft implementation of PPP CHAP. PPTP clients and servers are also supported by Linux and many major VPN products.

3.1.3 Layer Two Tunneling Protocol (L2TP)

L2TP is a combination of PPTP and L2F. Rather than having two incompatible tunneling protocols competing in the marketplace and causing customer confusion, the IETF mandated that the two technologies be combined into a single tunneling protocol that represents the best features of PPTP and L2F. Figure (6) shows that L2TP architecture divides the RAS functions between a L2TP Access Concentrator (LAC) that handles the physical communication to the remote client, and a L2TP Network Server (LNS) that terminates remote clients’ PPP session and acts as a gateway into the enterprise network [8].

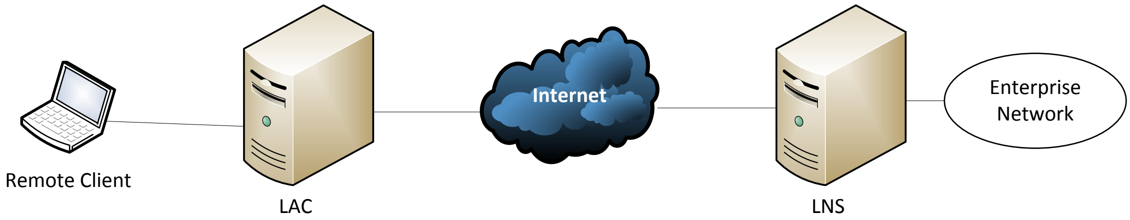

Figure 6: L2TP Architecture [8]

L2TP encapsulates PPP frames to be sent over IP, X.25, FR, or ATM networks. When sent over an IP network, L2TP frames are encapsulated as User Datagram Protocol (UDP) messages. L2TP uses UDP messages over IP networks for both tunnel maintenance and tunneled data. The payloads of encapsulated PPP frames can be encrypted, compressed or both. L2TP tunnel maintenance and tunneled data have the same packet structure as shown in Table (3) [8].

Data link header	IP header	UDP header	L2TP header	PPP header	PPP payload (IP datagram)	Data link trailer

Table 3: L2TP Packet Structure [8]

L2TP utilizes two types of messages, control messages and data messages. Control messages are used in the establishment, maintenance and clearing of tunnels and calls. Data messages are used to encapsulate PPP frames being carried over the tunnel. Control messages utilize a reliable Control Channel within L2TP to guarantee delivery. Data messages are not retransmitted when packet loss occurs.

L2TP-based VPN

L2TP has minimal built-in security that is used to provide data integrity, source authentication and replay protection. Like PPTP, L2TP depends on PPP to protect the user data in the tunnel. The overhead involved in providing this extra security results in a slightly slower performance than PPTP. In order to have strong security in place, the L2TP must be combined with an external security protocol. The most popular way of doing this is to run L2TP over Internet Protocol Security (IPSec). L2TP clients and servers are supported by most versions of Windows, Linux, and many major VPN products.

3.2 LAYER 3 Tunneling Protocols

These correspond to the Network Layer and uses packets as their unit of exchange. Internet Protocol Security (IPSec) tunnel mode operates at this layer and encapsulates the packets in an additional header before sending them across an IP network.

Internet Protocol Security (IPSec) IPSec is a framework of IETF open standards aim at securing traffic on the network layer. It does not specify the authentication and encryption protocol to use. This makes it flexible and able to support new authentication and encryption methods as they are developed [9].

IPSec Modes

IPSec has two methods of forwarding data across a network: transport mode and tunnel mode. Each differs in their application as well as in the amount of overhead added to the passenger packet. These protocols are summarized briefly in the next two sections: Tunnel mode encapsulates and protects an entire IP packet. Because tunnel mode encapsulates or hides the original IP header of the packet, a new IP header must be added in order for the packet to be successfully forwarded. Tunnel mode may be employed with either or both ESP and AH. Using tunnel mode results in additional packet expansion of approximately 20 bytes associated with the new IP header. Tunnel mode expansion of the IP packet is depicted in Table (4).

New IP header	IPSec header	Original IP header	TCP/UDP header + data

Table 4: Tunnel Mode

Transport mode works by inserting the ESP or AH header between the IP header and the next protocol or the transport layer of the packet. Both IP addresses of the two network nodes whose traffic is being protected by IPSec are visible in the IP header of the postencrypted packet. This mode saves an additional IP header, which results in less packet expansion. Transport mode can be deployed with either or both ESP and AH. Transport mode expansion of the IP packet is depicted in Table (5).

Original IP header	IPSec header	TCP/UDP header + data

Table 5 Transport Mode

Internet Key Exchange (IKE)

To implement a VPN solution with encryption, periodic changing of session encryption keys is necessary. IKE protocol is a key exchange and management system, which provide a secure key distribution services between parties wishing to communicate. IKE is a hybrid protocol composed of features from Internet Security Association and Key Management Protocol (ISAKMP), Oakley Key Determination protocol (OAKLEY), and Secure Key Exchange Mechanism (SKEME). IKE supports policy negotiation and establishment of authenticated keying material for Security Associations (SAs) [10].

Security Association (SA)

SA is an agreement between sender and receiver that defines a security relationship that include authentication algorithms and its keys, encryption algorithms and its keys, the

current sequence number, the anti-replay window, the lifetime of the SA and an identifying number, and the Security Parameter Index (SPI). Security associations control traffic in only one direction, bi-directional communication requires two security Associations. The set of related SAs are gathered into an SA bundle for easy handling during processing [9].
Security associations are held in a Security Association Database (SAD), where they can be retrieved during processing. SA is uniquely identified by Security Parameter Index (SPI), IP destination Address, and security protocol identifier [9].

A rule stating which datagrams should be sent through an IPSec VPN is called a Policy. In general, the policy is an action. That action can be to drop the datagram, to bypass the IPSec (transmit the datagram normally) or to apply IPSec protocols. The Security policy Database (SPD) is used to locate a policy to apply to a datagram, that policy points to the appropriate SA or SA bundle that implement that policy [9].

IPSec-based VPN

IPSec provides confidentiality, integrity, and authenticity of data communications across a public IP network. IPSec can be used as a complete VPN solution, or simply as the encryption scheme within L2TP or PPTP. IPSec is considered, by many, to be the standard VPN solution for site-to-site secure VPNs. IPSec is supported in Windows XP, 2000, 2003 and Vista, in Linux 2.6 and later. Many vendors supply IPSec VPN servers and clients. [11]
L2TP/IPSec combines L2TP's tunnel with IPSec's secure channel. Microsoft has provided a free L2TP/IPSec VPN client for Windows 98, ME and NT since 2002, and ships an L2TP/IPSec VPN client with Windows XP, 2000, 2003 and Vista. Windows Server 2003 and Windows 2000 Server include L2TP/IPSec servers. There are several open-source implementations of L2TP/IPSec for Linux [12].

3.3 LAYER 5 Tunneling Protocol

These correspond to the Session Layer and uses application datagrams as their unit of exchange. Secure Sockets Layer (SSL) operates at this layer and encapsulates the application datagrams in an additional header before sending them across an IP network.

Secure Sockets Layer (SSL)

SSL is a higher-layer security protocol developed by Netscape. It is used to, among other things, secure Hypertext Markup Language (HTML) transactions on the web. Most browsers and servers currently use SSL 3 [13]. SSL encapsulates application datagrams in the SSL record. When sent over an IP network, SSL records are encapsulated as TCP messages. SSL uses TCP messages over IP networks for both tunnel maintenance and tunneled data. SSL tunnel maintenance and tunneled data have the same record structure as shown in Table (6).

IP header	TCP header	SSL record header	SSL payload (application datagram)	SSL record trailer

Table 6: SSL Record Structure [13]

SSL Session

SSL session has three stages. In the connection setup stage, the authentication, encryption, and compression algorithms are negotiated, the identity of the server and client are verified, and a key exchange takes place. In the data transfer stage, the encrypted and authenticated application data are exchanged between client and server. In the connection tear down stage, the client and server or one of them send an authenticated closure notification when the applications have finished exchanging data.

All SSL messages are carried in SSL records. Figure (7) shows the general format of these records that contains the following fields [13]:

The Type field identifies the type of message. Table (7) lists the four message types. The Major and Minor version fields indicate the SSL version, SSL 3 has a major version of 3 and a minor version of 0. The Length field indicates the length in bytes of the payload data field. The Payload data field carries the message data.

The SHA1 HMAC is a cryptographically secure message authentication code that is used to provide authentication. The Padding and pad length fields are used to pad the message to the block size of the encryption algorithm.

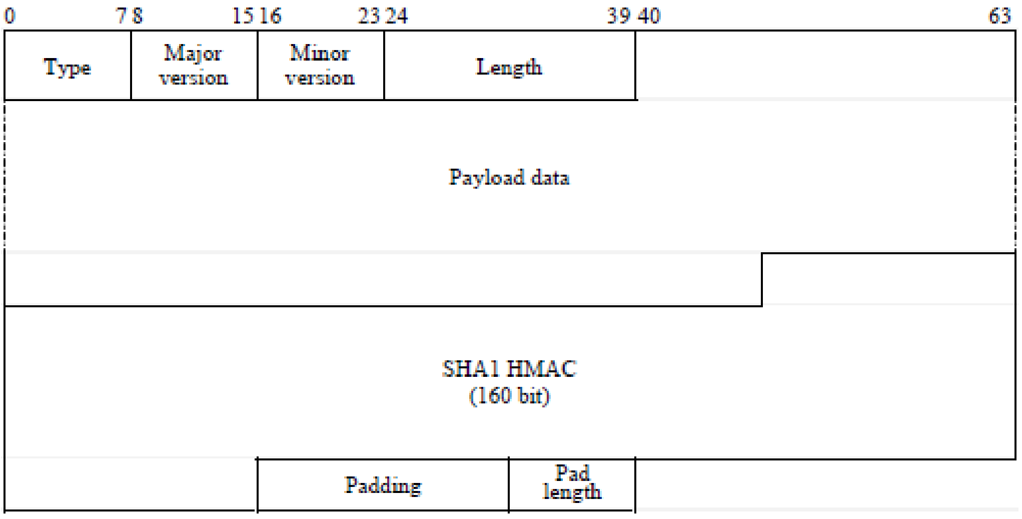

Figure 7: SSL Record Format [13]

Record type	Value	Description
CHAGE_CIPHER_SPEC	20	Switch to the last negotiated cipher
ALERT	21	Error or close notify messages
HANDSHAKE	22	Hello and other connection initiation
APPLICATION DATA	23	Data messages

Table 7: SSL Record Messages Types [13]

SSL-based VPN

SSL protocol was developed for transmitting private information across the Internet. It is commonly used with Hypertext Transaction Protocol (HTTP) to enable secure Web browsing, called HTTPS. Most browsers and servers currently use SSL 3.0 to provide confidentiality, integrity, and authenticity between web-client and web-server. However, SSL can also be used to create a VPN tunnel. For example, OpenVPN is an open source VPN package for Linux, BSD, Mac, Pocket PCs and Windows 2000, XP, 2003 and Vista, which uses SSL to provide encryption of both the data and control channels.

2.4 Label Switching Tunneling Protocol

This corresponds to inserting small label between the data-link layer and the network layer header. Multiple Protocol Label Switching (MPLS) encapsulates the IP packets in an additional label before sending them across an IP network.

Multiple Protocol Label Switching (MPLS)

MPLS is a label-based packet switching technique that has evolved from numerous prior technologies such as Cisco's "Tag Switching" and IBM's "ARIS". MPLS is independent of the Layer 2 and Layer 3 protocols which means that it supports numerous protocols both at the network layer (e.g. IPv6, IPv4, IPX, apple talk) and the link layer (e.g. Ethernet, ATM, Frame Relay). The idea is that a small label is inserted between the data link and network layer headers, as shown in Table (8) [14].

Data link layer header	MPLS label	IP header	TCP/UDP header + data

Table 8: MPLS Label Encapsulation [14]

The Label Edge Router (LER) operates on the edge of the network. The LER is responsible of assigning labels to the entering packets (ingress LER) and removing them from the existing packets (egress LER). The Label Switch Router (LSR) operates in the core of the network. The LSR is responsible of making forwarding decisions based on the context of the label and the incoming interface, and does not need to consult the network layer header at all.

In the MPLS network, each incoming packet is assigned to a particular Forward Equivalence Class (FEC) by the ingress LER. Class membership can be based on factors such as destination address, QoS requirements and the current state of the network. Each packet in a FEC will follow a predetermined path, called a Label Switch Path (LSP). LSPs allow placing high-priority traffic on the most expensive paths while allowing routine traffic to take other paths. This, in turn, guarantees a certain level of performance.

The MPLS label, as shown in Figure (8), is added to the packet. The label comprises a 20-bit Label value, an 8-bit TTL that's used to prevent routing loops, an S bit that, when set, indicates the bottom of the stack, and a 3-bit Exp field that will be used to provide differential service for MPLS. Packets can carry multiple labels arranged in a stack. Only the label at the top of the stack is used to route the packet. Other labels play no part until the top label is removed by one of the routers. The label determines what path (LSP) the packet will take through the MPLS network. After the label has been added to the packet, the packet is forwarded on the appropriate interface (i.e. the right LSP).

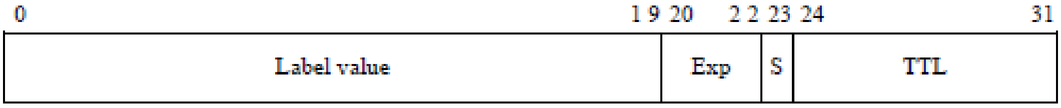

Figure 8: MPLS Label [14]

A table, specifying how each packet should be forwarded, is built by each LSR. This table is called the Label Information Base (LIB). When a packet arrives at an intermediary LSR, it retrieves the label and uses it as an index into local table. Each entry of the table contains at least next hope and a label forwarding action. Possible label actions are:

- Swap (replace the label at the top of the stack with another label).
- Pop (removing the top label and exposing the next label, if any).
- Replace (replace the label at the top of the stack with another label, and then push one or more additional labels onto the top of the stack).

The last router, i.e. the egress LER, finally strips the label of the packet and forwards the packet to an IP network using layer 3 routing. In order for LSPs to be used, the LIBs at each LSR must be populated with the correct mappings between incoming and outgoing interfaces and label values. This can be done by letting the LSRs distribute labels between them. The process is called label distribution. The MPLS architecture does not identify a specific method to distribute labels. Several distribution protocols are used to exchange label information, such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Label Distribution Protocol (LDP).

MPLS-based VPN

Since data is forwarded only based on the MPLS label, and not the rest of the payload, including the IP header, an LSP is considered to form a tunnel within the MPLS network.

MPLS provides a VPN solution based on the use of LSP tunnels. By labeling the VPN data as it enters such a tunnel, the LSR segregates the VPN flows from the rest of the data flowing in the MPLS network.

Scalability can be achieved by setting up LSPs inside LSPs, which gives very good multiplexing properties. Tunneling one LSP through another is simply a matter of adding another label to the “label stack” (the collection of labels attached to the packet). As the packet progresses, it is switched using the outer label. At the end of the LSP, the outer label is popped off, and the packet is switched using the new outer label.

Security can be guaranteed by assigning a unique label stack for each VPN destination. This ensures that data is not leaked out of the VPN. Any other traffic entered to the MPLS network (not destined for a specific VPN) is assigned a different label stack, ensuring that no data can be sent into the VPN by an unauthorized user. In addition, the MPLS routers can use cryptographic algorithms (e.g. MD5) if the service provider wants to protect the label distribution protocols from the insertion of fake labels or routers.

When creating MPLS-based VPNs, QoS can be assured by reserving network resources for the LSP tunnels. [14] This is good for a customer with a VPN based on MPLS, who can be sure of having a set amount of bandwidth.

4. CRYPTOGRAPHY

4.1 Introduction

The objective of a VPN is to allow two computers to exchange data in the same way, they do so on a LAN. Because we are working in a corporate environment these data are confidential and thus securing the data is important. By employing a VPN all the data exchanges exist in a public network. Everybody can eavesdrop on the data that two computers are exchanging. The public line does not give any guarantee to secure the data. This is the job of the VPN. It has to offer several services to assure the confidentiality and the integrity of the data : encryption and hashing.

Encryption makes it possible to encipher a message, so only the person who is allowed to read the message, can read the message. Hashing guarantees that the message is not modified during the transport of the message. [15]

4.2 Modern encryption methods

We can distinguish several cryptographic methods which deal with a VPN:

- Symmetric ciphers
- Asymmetric ciphers
- Message digests
- Digital signatures

Four important requirements have to be achieved for maximum security:

- Confidentiality: Only the person, to whom the message is sent, can read the message
- Integrity: Assuring that the message is not modified during transport.
- Authentication: Proving that the message is from the right person and not is modified by another person
- Non-repudiation: Assuring that once a message is sent, the sender cannot deny having sent the message and the receiver cannot deny having received the message

The non-repudiation of a message is an important requirement. For example in online bank transaction systems; once a transaction is performed, you cannot deny having carried out the transaction.

If we want to build a secure VPN, we have to assemble the four cryptographic methods to achieve the four objectives of data security.

4.3 Algorithms and keys

A cryptographic algorithm is a mathematical function that is used to encrypt and decrypt a message. An encryption algorithm encrypts plain text into ciphered text. The decryption algorithm decrypts the ciphered text into the plain text again.

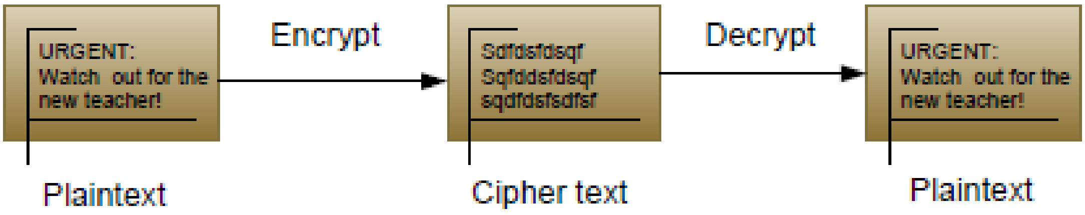
URGENT: Watch out for the new teacher!
Encrypt
Sdfdsfdsqf Sqfddsfdsqf sqdfdsfsdfsf
Decrypt
URGENT: Watch out for the new teacher!
Plaintext
Cipher text
Plaintext

Figure 9: Encryption and decryption of a message [15]

In order to explain the different algorithms some symbols need to be defined:

- plaintext = M
- ciphertext = C
- encryption algorithm = E(M)
- decryption algorithm = D(C)

All modern algorithms now use a key to encrypt and decrypt all messages.

- C = Ek(M) (Ciphertext is the encryption of the plaintext)
- M = Dk(C) (The plaintext is the decryption of the ciphertext)
- The following equation must always be true
- Dk((Ek(M)) = M

The security of the encrypted data depends on two elements:

- The invulnerability of the used algorithm.
- The confidentiality of the used key.

4.4 Symmetric algorithms

4.4.1 Objectives of symmetric algorithms

Symmetric algorithms assure the security of the exchanged data by using several mathematical transformations on the plain text message. All these transformations use the same key for encrypting and decrypting the message. We call this key the shared key. The sender and receiver of the message have to have the same shared key to encrypt and decrypt the message.

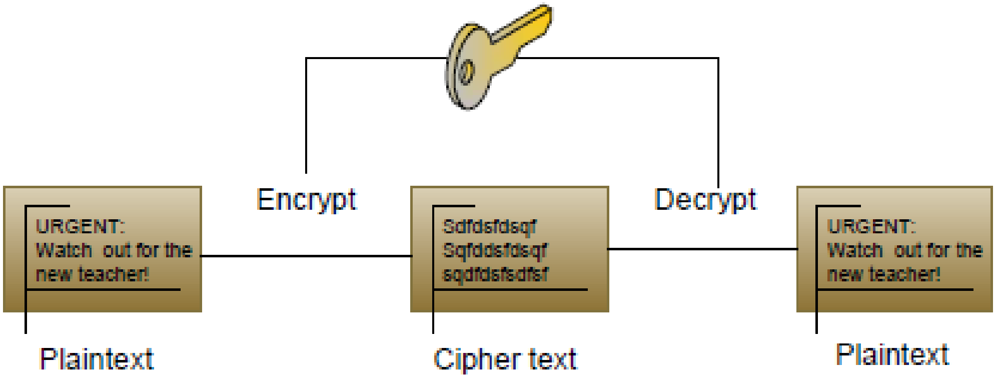

Figure 10: Symmetric algorithm with a shared key [15]

The key is distributed to the two communicating parties in a secure manner prior to the exchange of the encrypted data. Two of our goals are achieved, the confidentiality and authentication of the message. Confidentiality is assured because only the sender and receiver know the value of the shared key. The authentication is assured because the only one who can possess the key and thus cipher the message, is the sender of the message.

4.4.2 Possible attacks

4.4.2.1 Bruteforce attacks

A brute force attack is simply an attempt to try all possible cipher key combinations in order to find the one that unlocks the ciphertext. This is why this attack is also known as an exhaustive key search. The cracker makes no attempt to actually crack the key, but relies on the ability to try all possible key combinations in a reasonable amount of time. All encryption algorithms are vulnerable to brute force attacks.

This method is quite straight forward, we recover the right key to decrypt the ciphertext by trying every possible key combination. For example to crack a DES encrypted message, researchers managed to design a machine that could do it in less than three days. It depends simply on the computer power you have. By augmenting the key size, the algorithms become more robust. [15]

AES for example uses a 128 bit key, so it would take trillions of years to crack this key by brute force! We can thus say that AES is brute-force proof.

4.4.2.2 Cryptanalysis

Cryptanalysis is a science that tries to find flaws in the encryption algorithms in order to reduce the amount of keys that have to be tested. For example if we use an algorithm with a 128 bit key size and we can reduce the amount of possible keys from 2128 to

270. This weakens the algorithm considerably. [17] To date though, for AES, these flaws are only theoretical.

4.5 Asymmetric algorithms

4.5.1 Objectives of asymmetric algorithms

Asymmetric algorithms also called public-key cryptography assures the data exchange by using two different keys which are mathematically related. Both keys can be used to encrypt/decrypt a message. The ciphered text can only be decrypted by the key which is associated with the encryption key. [15] We distinguish two keys:

Public key: This key can be distributed to everybody, thus being public. This key is used to cipher a message to send to the owner of the private key. It can also be used to decipher a message from the owner of the private key.

Private key: This key is private and has to be kept secret. This key is used to decipher the message that is ciphered with the corresponding public key. It is also used to cipher a message that can be deciphered by the public key. Only the owner of the private key can read the messages encrypted with the related public key. It is imperative to keep the private key secret. The public key can be used to decrypt a message from the owner of the private key, in this way we can be sure that the message is sent by the right person. In figure (11) we see an example of a public key exchange.

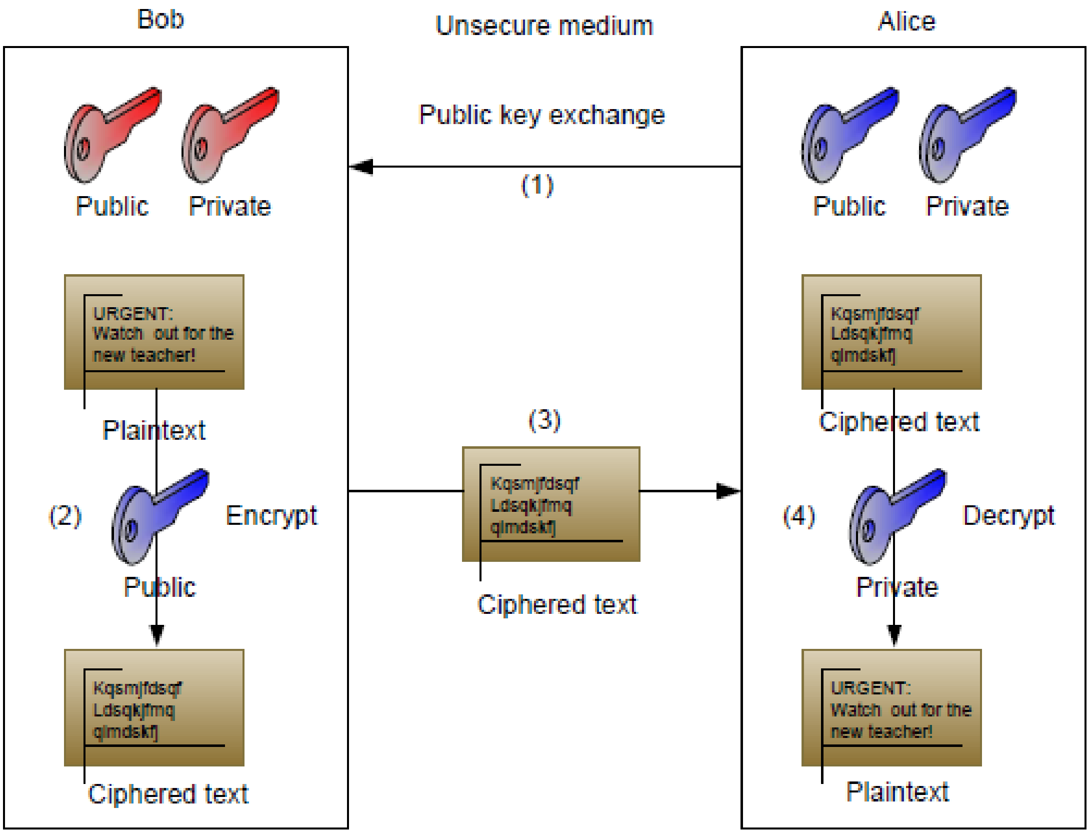

Figure 11: Asymmetric algorithm with a public/private key exchange [15]

1. Alice sends her public key to Bob over the unsecure medium
2. Bob uses Alice's public key to encrypt the message
3. Bob sends the encrypted message to Alice over the unsecure medium
4. Alice decrypts the message with her private key

4.5.2 Possible attacks

When cracking an RSA key, researchers try to find a method to guess the prime numbers needed to calculate the private key out of the public key. The length of the key is important. A key of 512 bits can be factored in 7 months. So a key size of at least 1024 bits is required, to have a secure key.

4.6 Comparison

We will now see that both algorithms, symmetric and asymmetric, can be used next to each other. Designers of security systems try to combine the advantages of both to obtain maximum security.

The speed of execution of the symmetric algorithms as well as the limited key size, needed to set up a secure communication, makes these algorithms well suited for file encryption. These algorithms are extensively used in securing VPN networks. A drawback is that the key for encryption and decryption is the same. As soon as one of the keys is compromised, you have to use another key, on both sides of the communication channel. To be secure you have to have a different pair of keys for every person you want to communicate with. Managing all these keys involves a lot of organization; the way to negotiate the pair of keys being a weak point in these algorithms. [15]

Public-key cryptography became public after Whitefield Diffie and Martin Hellman proposed the concept of an exponential key exchange scheme. The biggest advantage of this method is the way you can spread the public key without compromising your security. Everybody who wants to send an encrypted message to a specific person just uses that person's public key to cipher the message and only the person with the right private key can read the message. You only need one pair of public/private keys to exchange your data with a lot of people. You can set up a public database where everybody can get the public key of a person. The amount of keys necessary to communicate is much smaller and easier to manage. [15]

	Symmetric	Asymmetric
Advantages	Fast execution speed. Size of the ciphertext is limited	Keymanagement is easy to handle. Exchange of the public key is no problem.
Disadvantages	Keymanagement is exhausting. Exchange of the shared key has to be done in a safe way.	Slow execution speed because of bigger keysize. Encrypted message is bigger in size than the original plaintext.

Table 9: Advantages and Disadvantages

Another important fact is that the private key is the responsibility of the owner and not of two persons. Public-key cryptography also assures the non-repudiation of the messages. It is impossible to deny having sent the message afterwards. If a message is encrypted with the private key, all parties who have the public key can decrypt the message. In this way it proves that the message is sent by the owner of the private key, the origin of the message is proven.

We will combine both methods. For example we use the asymmetric algorithm to encrypt a random shared key and send this to our correspondent. The receiver can use this random shared key to encrypt his data using a symmetric algorithm and start communicating.

4.7 Hashing

Hashing is a special way of encryption. It is irreversible. The hashing algorithm generates a fixed unique hash-message (We call it a message digests) out of the original message. The size of the message does not matter. It is impossible to recover the original message out of the hash-message.

The hash message is considered as the digital fingerprint of the original message. It can be used to check if a message has been altered during transport. Because every hash is unique you always can detect if the integrity of the message has been changed. We can also guarantee the origin of the message by using hashing. [15]

The advantage of using a hashing algorithm is the fixed size of the message digest and the speed of execution.

4.7.1 Integrity control

4.7.1.1 How it works

When we send data over a public network, we do not know what will happen with our data. It can be changed by a pirate or by the equipment our data passes by. The moment we send our message we lose control of it. We can guarantee the integrity of our message by calculating a digital fingerprint of the message. By using hashing the receiver can control if something went wrong during transport.

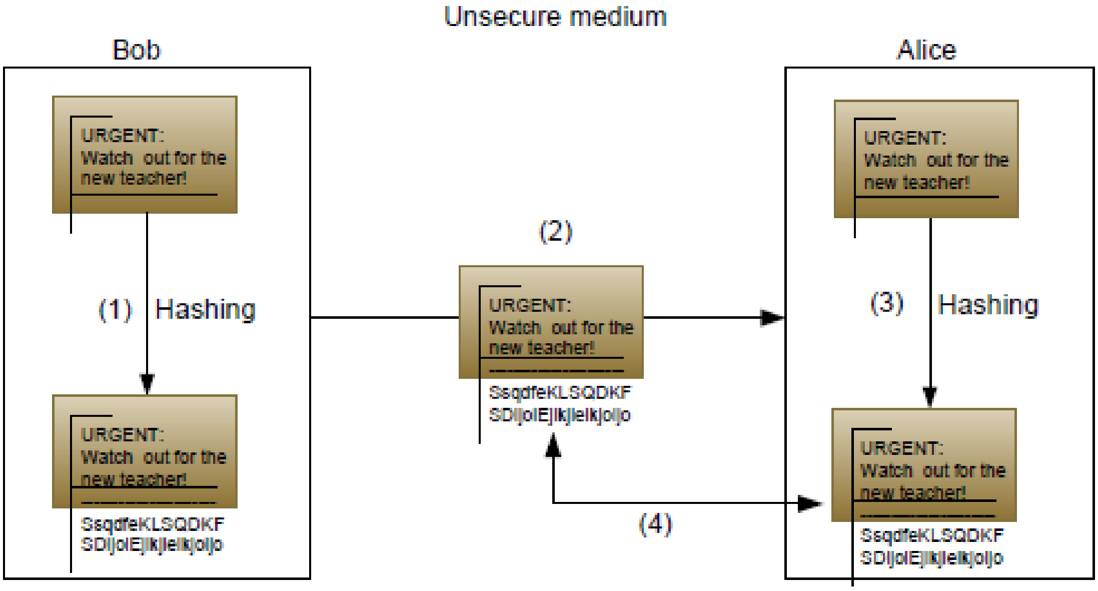

Figure 12: Concept of hashing [15]

1. Bob generates a hash of the message he wants to send.
2. Bob sends the message and the hash of that message.
3. Alice receives the message and generates a hash of the received message.

4. Alice checks if both the hashes are the same. If they are the same, the integrity of the message is assured.

4.7.1.2 Algorithms

A full explanation of all the hashing methods will not be given but the most important will be indicated, MD5 and SHA-1.

MD5 (Message Digest) Created by Robert Rivest, one of the inventors of the RSA algorithm. It is especially designed for 32-bit processors. The algorithm MD5 produces a 128-bit digest. MD5 is faster, but not as secure as SHA-1. [21]

SHA-1 (Secure Hash Algorithm) Created by NIST, SHA-1 is part of the U.S. Government's DSS standard, and works with DES to create digital signatures. SHA-1 produces a 160-bit message digest. [19]

The message digest produced by SHA-1 is bigger than MD5 and so it is better resistant against brute force attacks.

4.7.1.3 Possible attacks

To crack hashing algorithms, there are two possible methods:

- Finding collisions in the algorithm.
- Interception of the messages.

A hashing algorithm creates a unique digital fingerprint of a message. If we find a method that gives us the same fingerprint but calculated out of another message then the algorithm is not resistant to collisions. If we can create the same fingerprint for two different messages, then the security is wholly compromised.

Researchers discovered some flaws in the MD5 algorithm. Even by using a simple desktop Pentium computer they managed to produce two identical message digests out of two different messages.[1]. From that time on security experts have advised against using MD5. SHA-1 has a bigger message digest and is less vulnerable to collision attacks. The same group of researcher are trying to find flaws in SHA-1 but to date they have not succeeded. [19]

If we are using hashing mechanisms we are sure that the message is not altered during transport. But we are not sure who has sent the message. We cannot be sure about the origin of the message. An attacker can intercept the message and recalculate the message hash, because the hashing algorithms are public. To prevent this we have two options:

- Show the hash message on a website and after downloading the message, they can check if the hash message is the same as shown on the website.
- Another option is to make use of authentication methods to prevent the altering of the message hash by attackers.

4.7.2 Authentication

To assure the origin of a message we need to combine the hashing methods, which take care of the message integrity, and the encryption methods, which assure the confidentiality of the message. Two techniques are used in the context of VPN networks. Digital signatures by using RSA or DSS, and HMAC (Hashed message authentication code).

4.7.2.1 Digital signatures

Digital signatures are created by using one of the hashing methods, SHA-1 or MD5. First we produce a message digest out of the message. Later we encrypt this hash message with our private key. The receiver can read the hash message by using the corresponding public key. By comparing the message digest that the receiver calculates he can be sure that the message has been sent by the person from whom he possesses the public key. [20]

An important remark is the fact that we have to be sure that the public key we have received corresponds to the private key of Alice. If an attacker can intercept or change the public key and send us his public key, he can use his own private key to encrypt the message.

By using certificates we can assure that a particular public key is associated with the right private key.

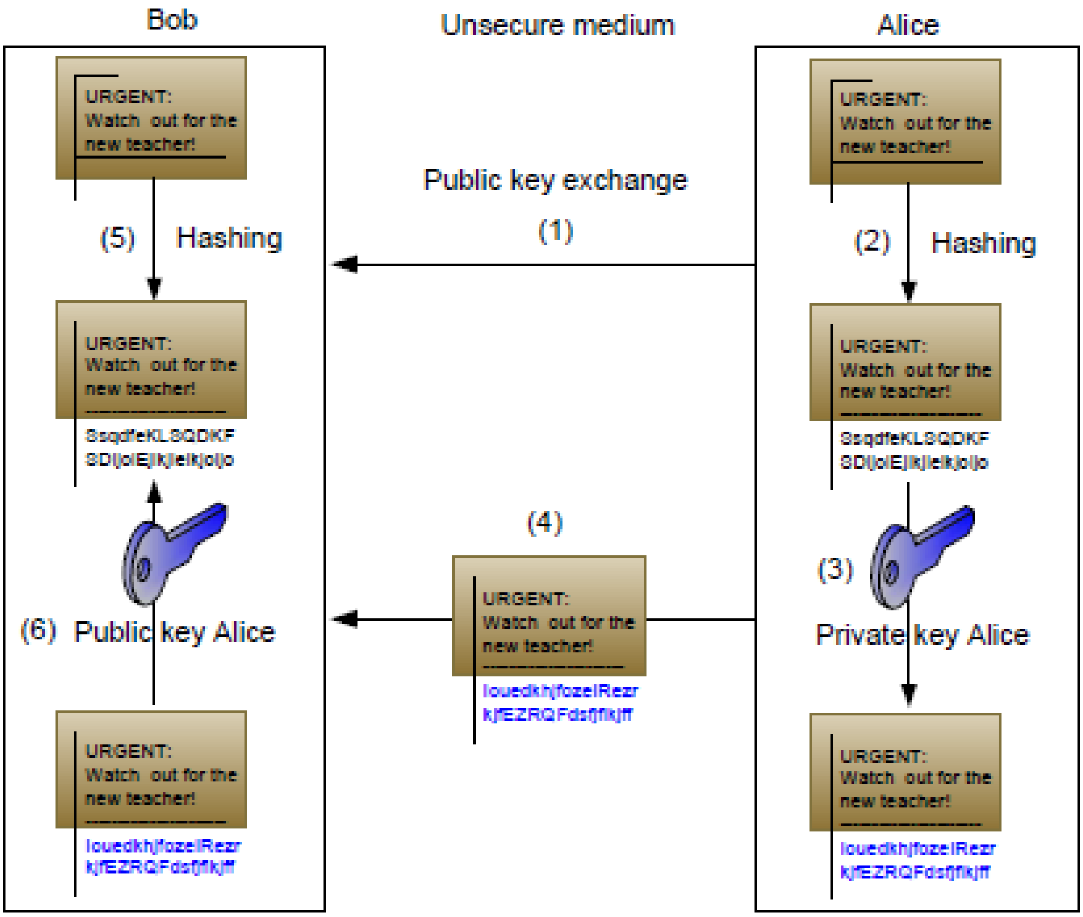
Bob
Unsecure medium
Alice
URGENT: Watch out for the new teacher!
Public key exchange
(1)
(5) Hashing
(2) Hashing
URGENT: Watch out for the new teacher!
SsqdfeKLSQDKF SDljolEjlkjlelkjoljo
(4)
(3)
(6) Public key Alice
Private key Alice
loued khjfozelRezr kjfEZRQFdsfjflkjff

Figure 13 Concept of a digital signature [15]

1. Alice sends her public key to Bob.
2. Alice produces a hash-message by using MD5 or SHA-1
3. Alice encrypts the hash-message with her private key.
4. Alice sends the message and hash-message to Bob.
5. Bob calculates the hash-message out of the received message.
6. Bob decrypts the hash-message of Alice by using her public key.
7. Bob compares if both hash-messages are the same.

5. IMPLEMENTING VPN IN SMALL TO MEDIUM SIZED ENETERPRISES

Small to medium sized enterprises often have more than one office, or they may have many branches managed and supported by a main office where all the systems are centralized. To spread out their services their branch offices has to have access to the centralized databases and applications; this must be done in the most secure and confidential way possible.

The solution for doing this is the establishment of virtual tunnels over the public networks such as the internet or so called Virtual Private Networks (VPN).

For a tunnel to be established, both the tunnel client and the tunnel server must be using the same tunneling protocol. Tunneling technology can be based on either Layer 2, Layer 3, Layer 5, or label switching tunneling protocol which are corresponding to the Open Systems Interconnection (OSI) Reference Model. [4]

IPSec is a framework of IETF open standards aim at securing traffic on the network layer. It does not specify the authentication and encryption protocol to use. This makes it flexible and able to support new authentication and encryption methods as they are developed [9].

AES is the result of a NIST initiation to develop a FIPS that specifies an encryption algorithm capable of protecting sensitive information, and is the standardized successor of the DES and 3-DES. NIST specifies that AES must support a block sizes of at least 128 bits and key size of 128, 192, or 256 bits. The AES keyspace is greater than 3-DES keyspace which provides AES with a greater resistance for a brute force search. Both the larger keyspace and the improved efficiency will probably put AES as the main encryption algorithm in all systems in a few years' time [15].

SHA was designed by the National Security Agency (NSA) and standardized by NIST in 1995. The design of SHA is similar to MD4 and MD5 that is described above. The SHA-1 algorithm takes a message of arbitrary length and produces a 160-bit message digest. The larger message digest space makes SHA more secure against a brute-force search than MD4 and MD5. The greater time complexity makes SHA more slower than MD4 and MD5 [19].

5.1 Proposed Solution

As mentioned above the microfinance institution needs a secure and confidential network between its main office and all the branch offices around the territory of Republic of Kosova.

The implementation of Virtual Private Network (VPN) will solve the problem of the micro finance institution. As explained in this thesis, there are many ways how a VPN can be implemented.

Based on the existing public (owned by private IPS's) infrastructure in Republic of Kosovo implementing a VPN over internet would not be much reliable and cost effective.

There are some ISP's offering VPN connections all around the territory through their network infrastructure.

My recommendation for the financial institution is to contract two different ISP's for Site to Site VPN in order to be good backed up and invest in active equipment which can be managed from the IT department. My recommendation regarding the type of VPN would be; site to site VPN using IPSec framework with pre-shared key authentication and AES encryption.

5.2 Proposed Topology

The proposed solution for the microfinance institution is, site to site VPN through an ISP infrastructure.

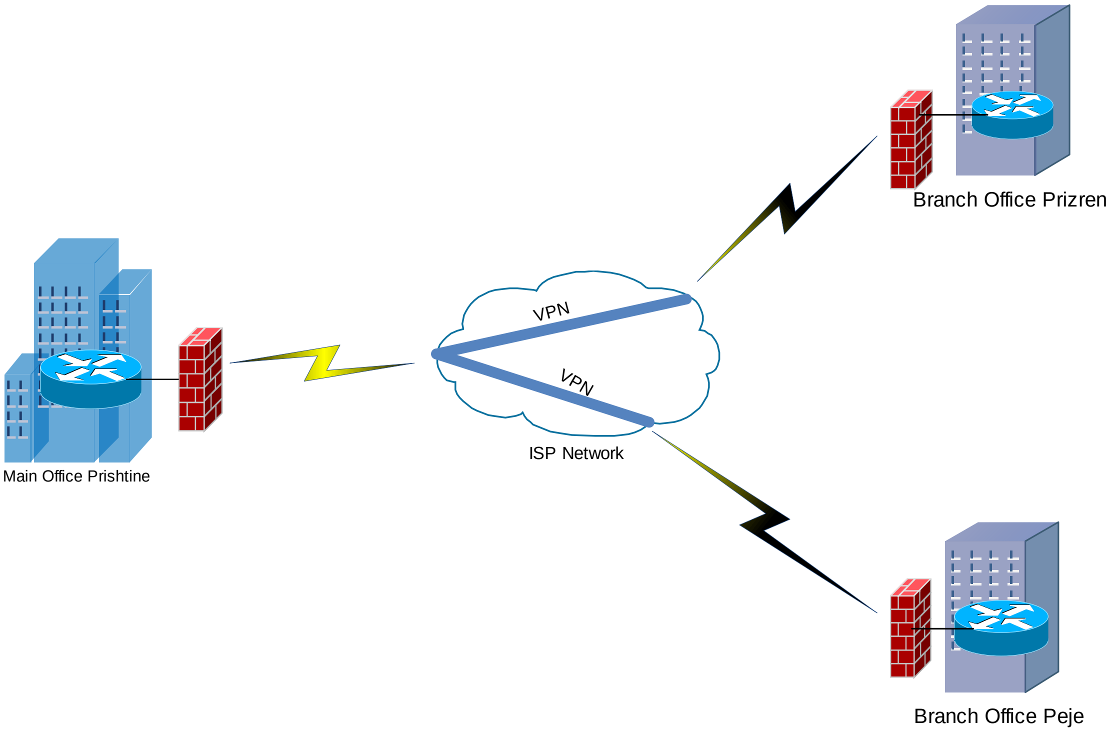

Figure 14: Proposed VPN Topology for the microfinance institution

6. SUMMARY

There are three different VPN types: access, intranet, and extranet. Access VPNs are used for remote users and normally require client software. Intranet and extranet VPNs are configured as site-to-site VPNs. VPN peers need to authenticate each other and negotiate the IPSec SA. The negotiation is completed automatically using IKE. The authentication is completed using preshared keys, RSA signatures (certificates), or RSA nonce. The user is able to choose between the cryptography methods available to make the VPN more reliable and confidential some of the methods: MD5, SHA, DES, 3DES, AES etc.

Advantages of a VPN:

- Low costs.
- Easy and fast implementation.
- Data assured by several encryption methods.
- Does not depend on the offered security of the ISP
- Easy to convert and very adaptable to new upcoming technologies.
- Easy access for roadwarriors.

Disadvantages of a VPN:

- Extra technical knowledge is necessary.

7. REFERENCES

[1] J. Lewis, and D. kahrs, “An Analysis of Virtual Private Networks,” Oregon State University, June 2004

[2] T. Collins, R. Keeley, and D. Waye, “Virtual Private Network: Definition,” whatis.com, May 2007

[3] http://en.wikipedia.org/wiki/Virtual_private_network, last visited: October 2012

[4] J. Snader, “VPNs ILLUSTRATED: Tunnels, VPNs, and IPSec,” Addison-Wesley, 2006

[5] W. Simpson, “Point to Point Protocol (PPP),” IETF RFC 1661

[6] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn, “Point to Point Tunneling Protocol (PPTP),” IETF RFC 2637, July 1999

[7] S. Hanks, T. Li, D. Farinacci, and P. Traina, “Generic Routing Encapsulation (GRE),”nIETF RFC 1701, October 1994.
http://www.ietf.org/rfc/rfc1701.txt, last visited: October 2012

[8] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter, “Layer Two Tunneling Protocol (L2TP),” IETF RFC 2661

[9] S. Kent, and R. Atkinson, “Security Architecture for the Internet Protocol,” IETF RFC 2401, November 1998
http://www.ieft.org/rfc/rfc2401.txt, last visited: October 2012.

[10] D. Harkins, and D. Carrel, “The Internet Key Exchange (IKE),” IETF RFC 2409,
http://www.ieft.org/rfc/rfc2409.txt, last visited: October 2012

[11] D. Shinder, “Comparing VPN Options,” WindowSecurity.com, Jun 2004.
http://www.windowsecurity.com/articles/VPN-Options.html, last visited: August 2012

[12] B. Patel, B. Aboba, W. Dixon, G. Zorn, and S. Booth, “Securing L2TP using IPSec,” IETF RFC 3193
http://www.ietf.org/rfc/rfc3986.txt, last visited: October 2012

[13] Freier, P.karlton, and P. Kocker, “The SSL protocol: Version 3.0 <draft-freier-ssl-version.txt>,” IETF RFC-DRAFT
http://www.ietf.org/rfc/rfc2547.txt, last visited: October 2012

[14] E. Rosn, Y. Rekhter, “BGP/MPLS VPNs,” IETF RFC 2547.
http://www.ietf.org/rfc/rfc2547.txt, last visited: September 2012

[15] Internet Security: Cryptographic principles, algorithms, Wiley, Man Youn Rhee, 2003

[16] S. Mister, S. Tavares, “Cryptanalysis of RC4-like Ciphers,” Lecture Notes in Computer Science, vol. 1556, PP. 131-143, Springer-Verlag, 1999
http://www.math.utah.edu/pub/tex/bib/toc/lncs1999a.html, last visited: September 2012

[17] NIST, “Data Encryption Standard (DES),” FIPS PUB 46-3, National Institute of Standard and Technology, October 1999
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, last visited: September 2012

[18] NIST, “Advanced Encryption Standard (AES),” FIPS PUB 197, National Institute of Standard and Technology, November 2002
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, last visited: October 2012

[19] NIST, “Secure Hash Standard (SHA),” FIPS PUB 180-2, National Institute of Standard and Technology, August 2002
http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf, last visited: October 2012

[20] NIST, “Digital Signature Standard (DSS),” FIPS PUB 186-2 (+Change Notice), National Institute of Standard and Technology, October 2001
http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf, last visited: October 2012

[21] R. Rivest, “The MD5 Message Digest Algorithm,” IETF RFC 1321, April 1992
http://www.ietf.org/rfc/rfc1321.txt, last visited: October 2012

[22] http://www.skapadmin.net

[23] http://blog.bartvpn.com

[24] http://www.cisco.com

7. APPENDIX

7.1 VPN Configuration Script

This may be a configuration option for a site to site VPN for the microfinance institution.

Site to site VPN configurations of the Prishtina and Peja sites through IPSec GRE Tunneling with Pre-shared key authentication method and AES 256 encryption.

PRISHTINA ROUTER

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key PRN address 10.254.164.254
!
!
crypto ipsec transform-set TRANS-SET-TUNNEL esp-aes esp-sha-hmac
!
crypto map CRYPTO-MAP 1 ipsec-isakmp
 description *** PRI_VPN_RTR ***
 set peer 10.254.164.254
 set transform-set TRANS-SET-TUNNEL
 match address IPSEC-TRAFFIC
!
!
interface Tunnel10
 description ***VPN_TO_PEJA***
 ip address 10.10.77.1 255.255.255.252
 ip mtu 1420
 tunnel source FastEthernet0/0
 tunnel destination 10.254.164.254
 crypto map CRYPTO-MAP
!
!
!
interface FastEthernet0/0
 description ***Link to ISP***
 encapsulation dot1Q 30
 ip address 10.254.30.86 255.255.255.252
 crypto map CRYPTO-MAP
!
interface FastEthernet0/1
 description ***Link to Core***
 ip address 192.168.0.201 255.255.255.252
 no ip redirects
 duplex auto
 speed auto
!
router eigrp 192
 network 192.168.0.0 0.0.255.255
 no auto-summary
!
ip classless
ip route 10.254.164.254 255.255.255.255 10.100.30.85
ip route 192.168.99.0 255.255.255.0 Tunnel10
ip http server
no ip http secure-server
!
ip access-list extended IPSEC-TRAFFIC
 remark VPN_Traffic
 permit gre host 10.254.30.86 host 10.254.164.254
```

PEJA ROUTER

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key PRN address 10.254.30.86
!
!
crypto ipsec transform-set TRANS-SET-TUNNEL esp-aes esp-sha-hmac
!
crypto map CRYPTO-MAP 1 ipsec-isakmp
 description to PEJA_VPN_RTR
 set peer 10.254.30.86
 set transform-set TRANS-SET-TUNNEL
 match address IPSEC-TRAFFIC
!
!
interface Tunnel5
 ip address 10.10.77.2 255.255.255.252
 ip mtu 1420
 tunnel source FastEthernet0/0
 tunnel destination 10.254.30.86
 crypto map CRYPTO-MAP
!
interface FastEthernet0/0
 description ***Link TO ISP***
 ip address 10.254.164.254 255.255.255.0
 duplex auto
 speed auto
 crypto map CRYPTO-MAP
!
```

```
interface FastEthernet0/1
 description LAN
 ip address 192.168.99.1 255.255.255.0
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.254.164.1
ip route 192.168.0.0 255.255.0.0 Tunnel5
ip http server
no ip http secure-server
!
ip access-list extended IPSEC-TRAFFIC
 remark VPN_Traffic
 permit gre host 10.254.164.254 host 10.254.30.86
!
```

7.2 List of Abbreviations

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AH	Authentication Header
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
DES	Data Encryption Standard
DSA	Digital Signatures Algorithm
DSS	Digital Signatures Standard
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECP	Encryption Control Protocol
ESP	Encapsulation Security Payload
FR	Frame Relay
GRE	Generic Routing Encapsulation
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IPX	Internet Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
LAC	L2TP Access Concentrator
LAN	Local Area Network
LCP	Link Control Protocol
LDP	Label Distribution Protocol
LER	Label Edge Router
LIB	Label Information Base
LNS	L2TP Network Server
LSP	Label Switch Path
LSR	Label Switch Router
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
MAC	Message Authentication Code
MD4	Message Digest algorithm 4
MD5	Message Digest algorithm 5
MPLS	Multi-Protocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft Challenge Handshake Authentication

	Protocol
NCP	Network Control Protocol
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OAKLEY	Oakley Key Determination protocol
OSI	Open System Interconnection
OSPEF	Open Shortest Path First
PAC	PPTP Access Concentrator
PAP	Password Authentication Protocol
PKI	Public Key Infrastructure
PNS	PPTP Network Server
PE	Provider Edge
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RAS	Remote Access Server
RSA	Rivest Shamir Adleman
RSVP	Reservation Protocol
SA	Security Association
SAD	Security Association Database
SHA	Secure Hash Algorithm
SKEME	Secure Key Exchange Mechanism
SLA	Service Level Agreement
SPD	Security Policy Database
SPI	Security Parameter Index
SSL	Secure Sockets Layer
SP	Service Provider
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Data Protocol
VPN	Virtual Private Network
WAN	Wide Area Network