Fall 10-2013

VPN- Virtual Private Network

Dallandyshe Gutaj

University for Business and Technology
School of Computer Sciences and Engineering

VPN- Virtual Private Network

Bachelor Degree

Dallandyshe Gutaj

Tetor / 2013

Universities for Business and Technology
School of Computer Sciences and Engineering

Bachelor Thesis
Year 2009 – 2010

Dallandyshe Gutaj

VPN- Virtual Private Network

Mentor: Selman Haxhijaha

Tetor / 2013

Bachelor Degree

ABSTRACT

In my thesis there is about Companies which I`m working, Bechtel- Enka GP uses VPN, Cloud Computing, and Data which are used Qos and Security. The Virtual Private Network which uses Bechtel-Enka is between a Venture Joint in Kosovo not between their selves.

Because the station of servers and network is in Camp Zhur all other links are used by via Kukes VPN, Prishtina Office VPN to Camp Zhur and via Suhareke to Camp Zhur. There is in use just a Server for all these relationship.

Outlook is used by all workers which share data for whole company. Phones also are included by them utilizing servers which are used for different works, one of them is using for sharing data for whole company using outlook and the other one for phones which are used intern and roaming calls.

Similarly, open source software enables IT departments of a Project to quickly build and deploy applications, but at the cost of control and governance. Finally, virtual machine attacks and Web service vulnerabilities existed long before cloud computing became fashionable. Indeed, this very overlap is reason for optimism; many of these “cloud problems” have long been studied and the foundations for solutions exist.

Security in today’s environments is established using strong authentication, authorization, and accounting procedures, establishing security of data at rest and in transit, locking down networks, and hardening operating systems, middleware, and application software. Surely, a general scenario has been defined. The project has also a remote office in Zhur camp so an employee has the related access to the corporate intranet. Depending on the Project requirement, the IS&T Engineers within contact with Management team have to decide the best technology is and have to be used by employees staff.

ACKNOWLEGEMENT

Indeed, what I did till now it's a work of me but a help of my family.

First of all I want to let you know that this way as huge as it was it has also different difficulties. I want to thank especially my family whom gave the powerful time to me in different cases support and take care over me, my friends Pelin, Neslihan, Ramadan,Narta, Sezin, Erinda and all the ones who help me in their psychologically way. It was not such easy to come to the end.

Thank you is very respectful word; this is all what I had to say.

Table of Contents

TABLE OF FIGURES:

GLOSSARY OF TERMS

This section provides a brief review of some of the VPN related terminology used in the thesis.

Email Server	An application that controls the distribution and storage of e-mail messages.
Firewall	A firewall is a program that protects the resources of one network from users from other networks.
Gateway	A gateway is a network point that acts as an entrance to another network.
HTML	A standard set of commands used to structure documents and format text so that it can be used on the Web.
Http	HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
Ip	The Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet.
Packet	A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.
Private Key	In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, the communicators would share a key so that each could encrypt and decrypt messages.
ISDN	Integrated Services Digital Network A set of communications standards allowing a single wire or optical fiber to carry voice, digital network services and video .
Key Management	The establishment and enforcement of message encryption and authentication procedures, in order to provide privacy-enhanced mail (PEM) services for electronic mail transfer over the Internet.

Protocol	A special set of rules for communicating that the end points in a telecommunication connection use when they send signals back and forth.
Proxy	An agent that acts on behalf of a user, typically accepting a connection from a user and completing a connection on behalf of the user with a remote host or service..
Public Key	A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.
QoS	QoS is the set of techniques to manage network resources.
Session	In the Open Systems Interconnection (OSI) communications model, the Session layer (sometimes called the "port layer") manages the setting up and taking down of the association between two communicating end points that is called a connection.
VPN	A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together.
Bandwidth	is directly proportional to the amount of data transmitted or received per unit time
Domain	The unique name used to identify an Internet network
Email client	An application from which users can create, send and read e-mail messages.
Email server	An application that control

1. INTRODUCTION

This is thesis which I used to explain about the company which I`m working. Bechtel-Enka is the company that has the biggest work to do in Kosovo in a Project of motorway. Indeed, within technology which they used they do their job as well as possible, within all procedures which are required, are utilized and provided by every worker for a better performance, quality and willing to cost and time.

The network within walls is a private network that only are authorized users related to the departments as they needed can access and work with, while the Internet is available for everyone's use within websites which are closed for Company benefits. Without proper precautions, the Internet can be a dangerous place for a company to live our assets, customer data, control systems can all be exposed to unauthorized users if they use the Internet as a communications system. We say that VPNs have the capability to connect networks, for example the host-network or network-network VPN scenarios.

Figure 1: VPN structured [1]

All VPNs have two hosts that handle the encryption/decryption of the VPN traffic, the endpoints of the VPN. When one or both of these hosts allows access to a network of machines rather than to just the single host, we call the host a *gateway*. The concept of a gateway is already standard networking terminology. For example, the router that connects a business to its ISP is a gateway, as could be a firewall through which all traffic passes. In VPN terminology, a gateway is simply a VPN endpoint that sits in front of a network that has access to the VPN. That is where the power of VPN comes in [3].

VPN transforms the communications systems of the Internet into a *virtual* private network for your company's use. The department of IS&T is supposed to provide and work with every technology with their knowledge's for a better work. What they do?

The main office, which is in Camp Zhur, has the whole servers that are used for different jobs. The departments and other technologies that are required link computers. Also, every office- worker to share their information's between each other for a better solution uses mobile phones. There are used also mobile phones for roaming calls for Procurement, Contracts, H&R, departments which have to do their obligations into Company.

1.1 Research questions

1.1.1 The way of creating VPN

Figure 2: Set up a VPN connection [2]

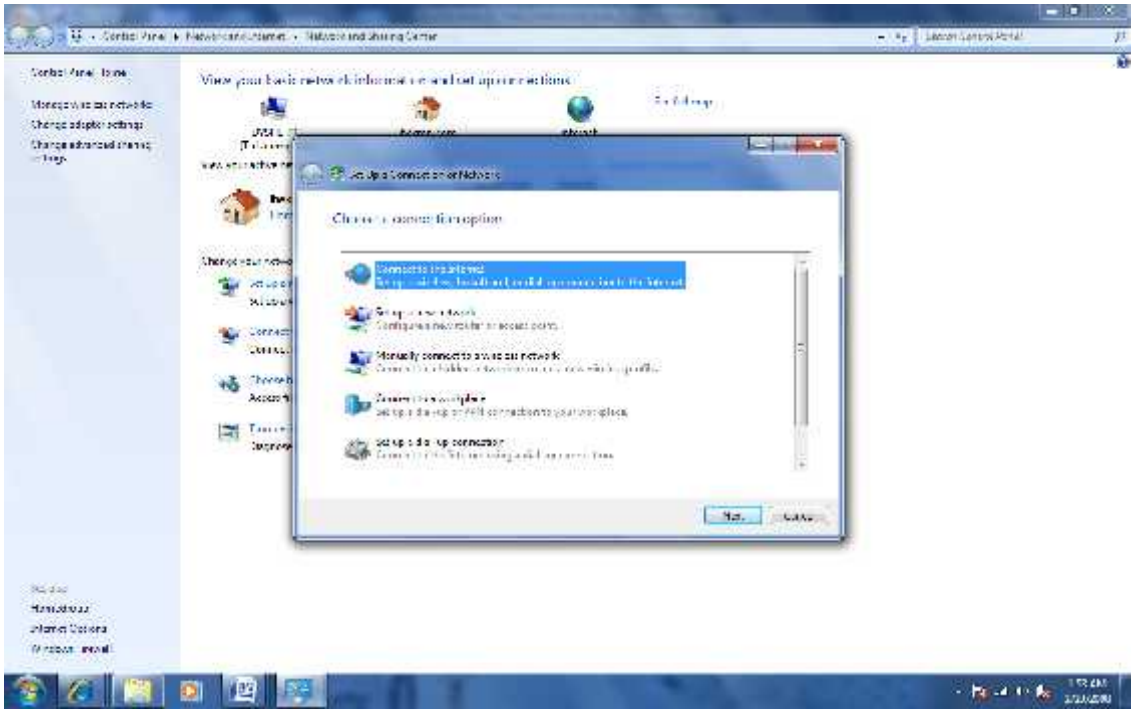

Figure 3: Connect to an Internet [3]

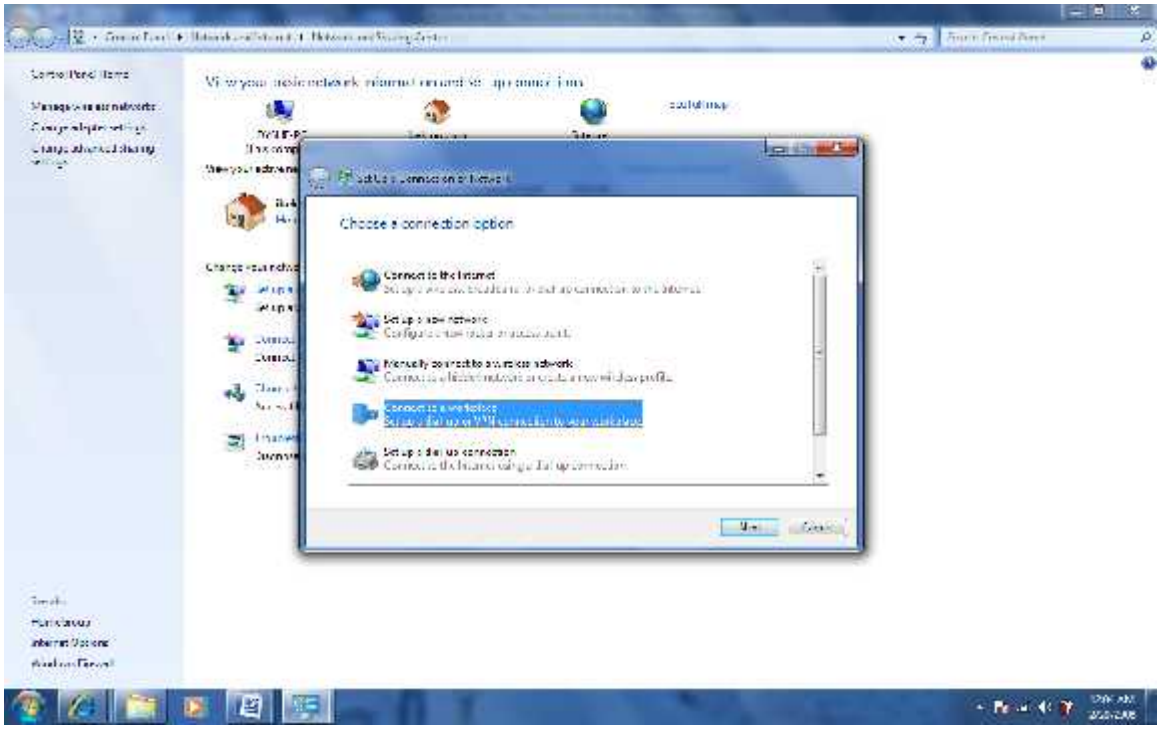

Figure 4: Connect to a workplace within VPN [4]

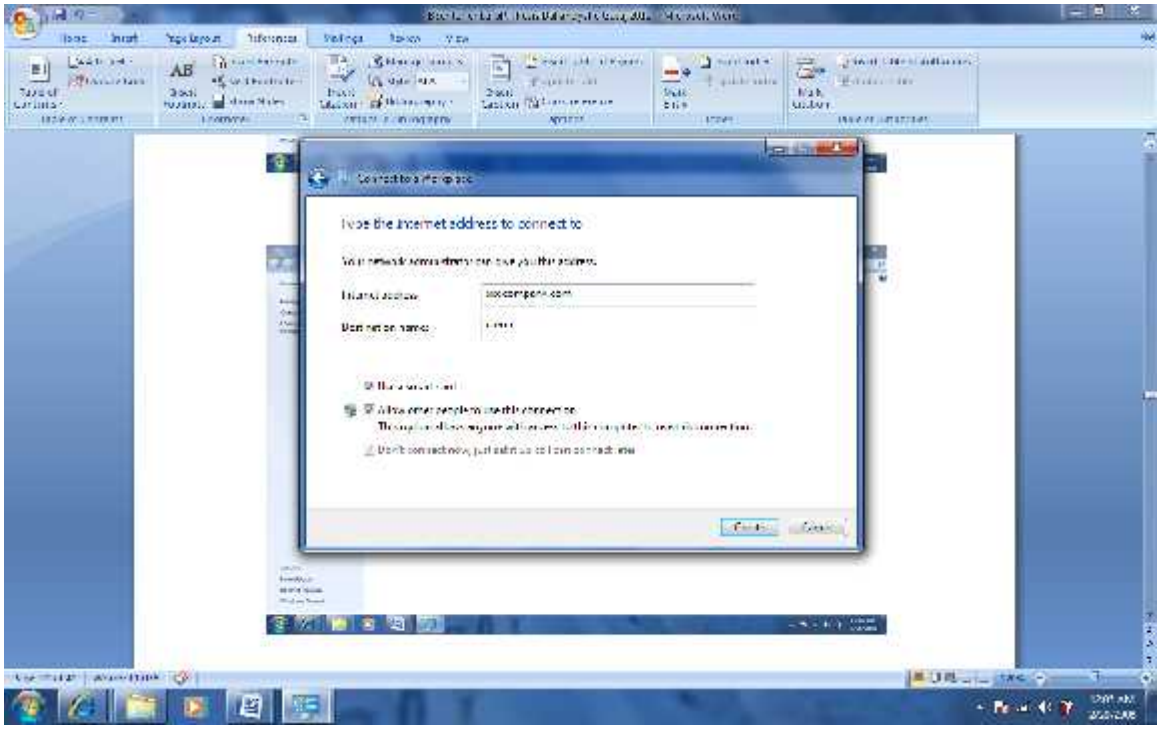

Figure 5: Writing the company name and allowing whom [5]

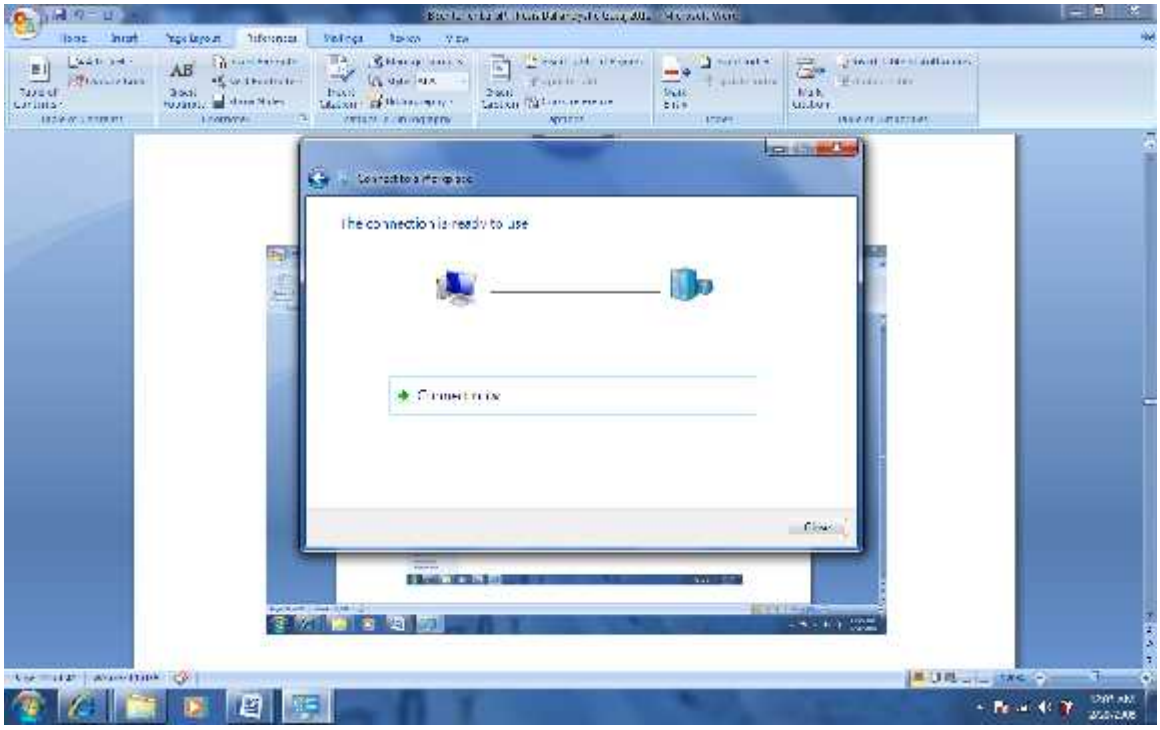

Figure 6: The connection is in a way [6]

1.2.1 Configuring the VPN Server

It`s not such easy to configure one Server, the way that Bechtel- Enka GP configure the server as not as different from the other companies do. So, I thought that the way that Cisco do is as same as we do in our Motorway Project as it is described below: Cisco has defined the following seven steps to configuring the Easy VPN Server:

- ✓ Enable policy lookup via AAA.
- ✓ Define group policy for mode configuration push.
- ✓ Apply mode configuration and Xauth to crypto maps.
- ✓ Enable Reverse Route Injection (RRI) for the VPN Client (optional).
- ✓ Enable IKE Dead Peer Detection (optional).

- ✓ Configure RADIUS server support (optional).
- ✓ Verify the Easy VPN Server.

Each step itself consists of multiple steps. Step 1 involves enabling AAA. Steps 2 and 3 involve configuring IPSec. Steps 4 through 6 are specific to Easy VPN Server configuration, but as mentioned previously, they're optional. Finally, in step 7, the show crypto map *interface* command can be used to verify Easy VPN Server operation [14].

Figure 7: Launching VPN Client [7]

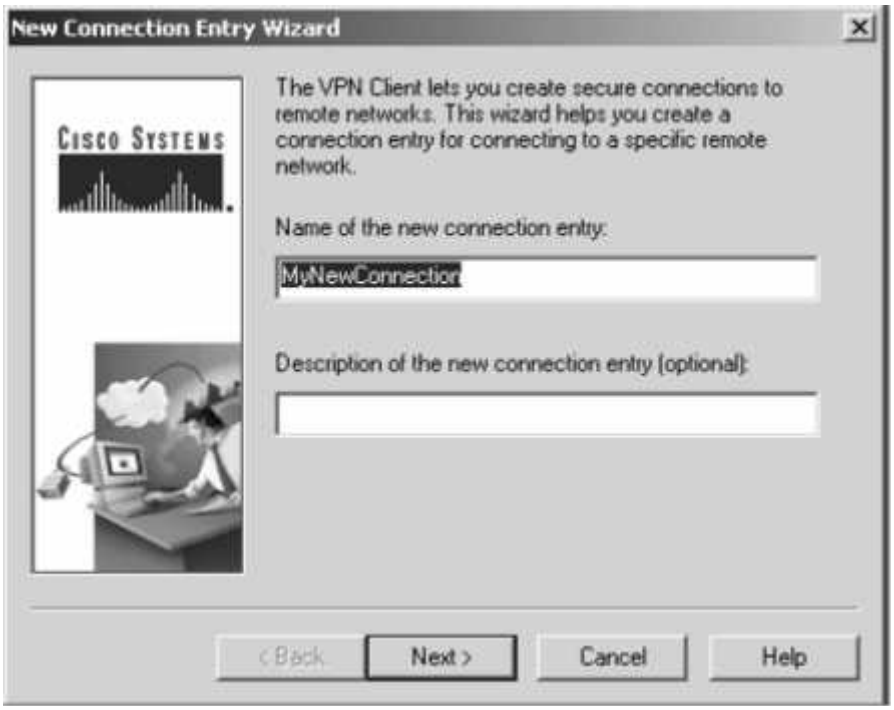

Figure 8: Creating a new connection entry [8]

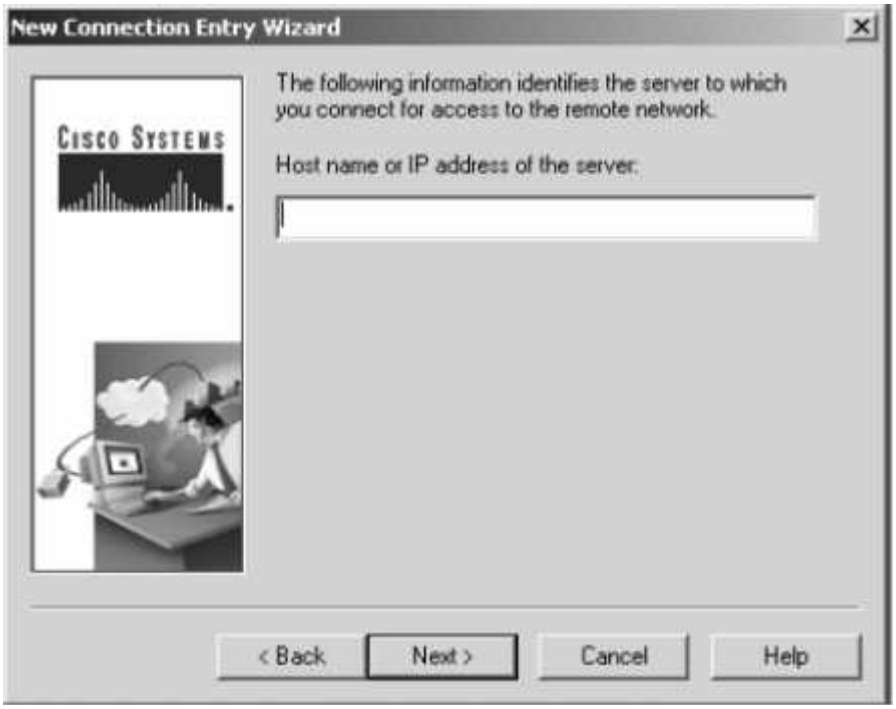

Figure 9: Identifying the VPN server to be connected [9]

Figure 10: Entering group access information [10]

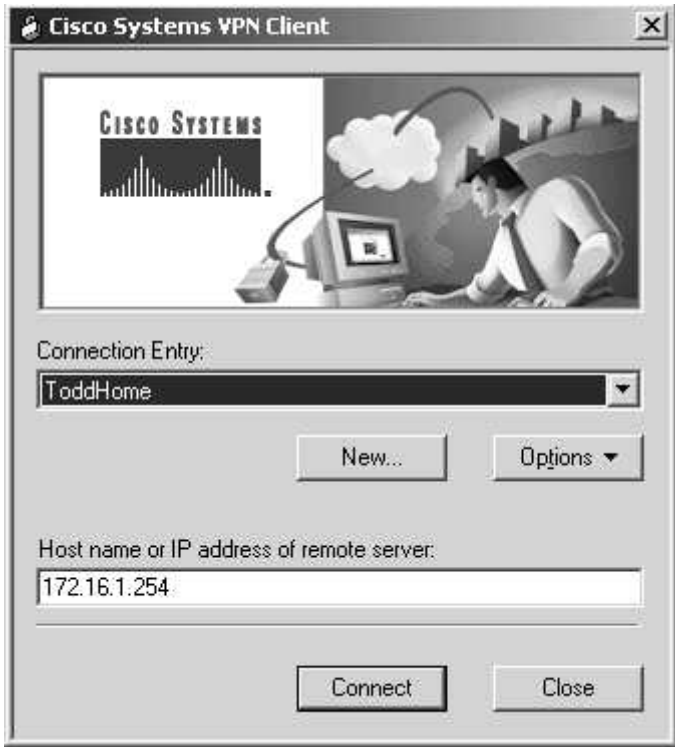

Figure 11: Connecting your VPN server [11]

1.2.2 Configuring Your VPN with Its Own Firewall

In any of the configurations previously described, it is possible to restrict what traffic can traverse the VPN connection. This might be desired when the networks or hosts you are connecting are not of the same trust level. For the case in which your Internet firewall and VPN server is the same machine, this can be achieved simply by adding new rules to the firewall using your existing firewall software.

For cases when you have a separate VPN server, you might either install a separate firewall machine in front of your VPN server or simply rely on Linux kernel packet filters on the VPN server. For example, if you want to allow only mail-related traffic to traverse your VPN, you might implement kernel restrictions on your VPN server, such as the following:
Allow only SMTP, POP, IMAP and POPs/IMAPs through our VPN:

```
for port in 25 109 110 143 993 995 do
ipchains -A output —destination-port $port -i vpn1 -j ACCEPT
ipchains -A input —source-port $port -i vpn1 -j ACCEPT
done
ipchains -A output -i vpn1 -j DENY
ipchains -A input -i vpn1 -j DENY
```

These rules assume that your VPN traffic goes through the virtual interface vpn1.This is a very simple example. You can create ACLs tailored for your VPN using whatever tools (IPchains, IPtables, IPfilter, and so on) you are comfortable with.

2.0 Literature Review

2.1 Bechtel Enka using Qos and Security

Bechtel is among the world's premier engineering, construction, and project management companies. Since its founding in 1898, Bechtel has worked on more than 22,000 projects in 140 countries and all seven continents. Bechtel is a global leader in developing, managing, and constructing civil infrastructure, from highway, airport, and rail systems to regional development programs. Today, its 49,000 professional and craft employees are teamed with customers, partners, and suppliers on hundreds of projects in nearly 50 countries [3].

Figure 12: The background of Bechtel Company [12]

Enka has 37 subsidiaries engaged in a diverse range of construction activities including power generation, airports, petroleum, and roadways. Enka primarily operates in Turkey, the Commonwealth of Independent States, North Africa, and Europe [1].

The Bechtel-Enka GP will be responsible for design management, procurement, and construction. The project will maximize opportunities to benefit the local economy through the use of local contractors, suppliers and employment on the project. Work is expected to begin in April 2010. Working as an integrated team, the Bechtel-Enka JV has successfully completed infrastructure projects across Europe and Asia that include more than 28,000

kilometers of highways and roads, 100 tunnels, and 25 major bridge projects [3].

QoS refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying Technologies. Primary goals of QoS include dedicated bandwidth, controlled jitter and latency (Required by some real-time and interactive traffic), and improved loss characteristics.

QoS-Technologies provide the elemental building blocks that will be used for future business applications in campus, WAN and service provider networks. This chapter outlines the features and benefits of the QoS provided by the Cisco IOS QoS.

In late 90s or even now, ask any web developer, solution architect or anyone involved in web application development in any capacity:

Which symbol do you use to represent Internet on numerous white-board meetings? Obviously the most widely used metaphor for Internet was/is cloud. Cloud computing has derived its name from the same line of thinking.

Security: As the Internet is a public network with the security risks associated with the open transmission of data, companies that rely on Internet VPNs depend on the encryption of their data to prevent the threat of security violations, such as spoofing, sniffing or man-in-the-middle attacks. A VPN is thus considered a Virtual "Private" Network since user data transmitted over the link is typically encrypted. Windows 95/98/NT/2000 based networks achieve this security via Microsoft's own Point-to-Point Encryption protocol, or MPPE. This encryption method was developed especially for use with the protocol PPTP, a major tunneling protocol.

Cloud Computing is a *style of computing that* must cater to the following computing needs:

Dynamism - Your business is growing exponentially. Your computing need & usage is getting bigger with every passing day. Would you add servers & other hardware to meet the new demand?

Assume, Recession is back & your business is losing customers. The servers &hardware you added during last quarter's peak season is now idle. Will you sale them? Demand keeps on changing based on world/regional economy, sometimes seasonal traffic burst as well. That's where Cloud Computing comes to your rescue! You just need to configure & your provider will take care of fluctuating demand.

Abstraction- Your business should focus on your core competency & should not worry about security, OS, software platform, updates and patches etc. Leave these chores to your provider. From an end users perspective, you don't need to care for the OS, the plug-ins, web security or the software platform. Everything should be in place without any worry.

Resource Sharing- Resource sharing is the beauty of Cloud Computing. This is the concept which helps the cloud providers to attain optimum utilization of resources. Say, a company dealing in gifts may require more server resources during festive season. A company dealing in Payroll management may require more resources during the end or beginning of the month.

A VPN is the extension of a private network that encompasses links across shared or public networks such as the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. In essence, it makes the remote computer virtually part of the private network by making an encrypted tunnel through the public Internet. The act of configuring and creating a VPN is known as virtual private networking [9].

Virtual private networks (VPNs) are also considered trusted networks, only they send data across 'untrusted' networks. So they're special—they create special circumstances and

require special considerations in establishing a security policy for them. The packets transmitted on a VPN are established on a trusted network, so the firewall server needs to authenticate the origin of those packets, check for data integrity, and provide for any other security needs of the corporation [18].

What features are needed in a well-designed VPN? It should incorporate:

· Security
· Reliability
· Scalability
· Network management
·Policy Management.

A well-designed VPN can greatly benefit a company such as Bechtel-EnkaGPdoes. Including: Extend geographic connectivity, Improve security, Reduce operational costs versus traditional WAN, Reduce transit time and transportation costs for remote users, Improve productivity, Simplify network topology, Provide global networking opportunities, Provide telecommuter support, Provide broadband networking compatibility, Provide faster ROI (return on investment) than traditional WAN.

2.2 Quality of services using Internet

This is 21`rst century and the life which we are living could not be imagined if there is not Internet. So, we can say that everything is up to the Internet. In this case it has been looked for a better solution and to be near the best way of applications, which could be done in the way that level which can be persecuted.

- Law latency
- Law lost
- Save of bit sequences for real –time applications

- Till now the Quality of Service offers just `Best- effort` service which pretend to be the best one because this one was not usable as pretend to be. Another words, this is not enough for the capacity that has.
- QoSis quite good linked within network, with the priority and with the control of latency of Network applications.

In reality, the level of quality is equal with the worst quality in between offers and requesters. It was used to argue about what could be done for a better Quality of Service.

Better Capacity. This is a choice that enables small delays and different priorities in network not at the expense of lower applications.

This is applicable for the networks that are not such loaded. For networks with are loaded more as considering the heterogeneity of applications, this solution can`t be long after the Network will still be overburdened by rapid movement of packets through different paths.

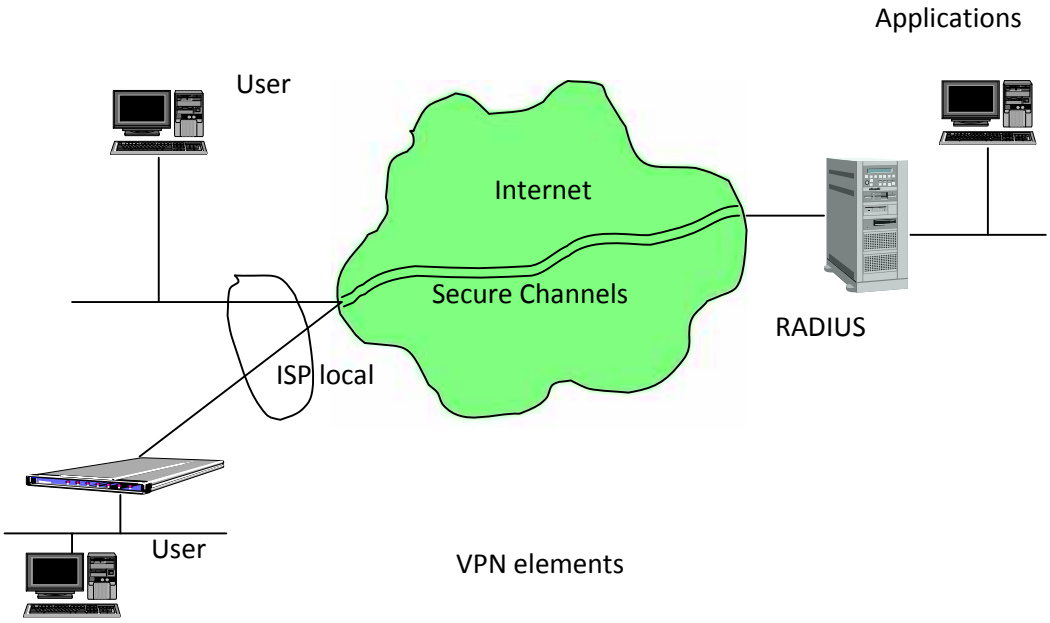

Figure 13: VPN elements [13]

We know that until now there has always been a clear division between public and private networks. A public network, like the public telephone system and the Internet as company use is a large collection of unrelated peers that exchange information more or less freely with each other.

VPN connections allow users working at home or on the road to connect in a secure fashion to an organization's remote server by using the routing infrastructure provided by a public internetwork (such as the Internet). Definitively, we can say that we open our eyes in front of it and for sure are quite closer to our job.

Workers in a Project Motorway with access to the public network may or may not have anything in common as departments are. For example Procurement department, Subcontract Department, Control Project, Engineering has to be shared data that they work for. As you focus on sharing more and more information so that everyone from related departments can get what they need, you must also remain focused on the security of that information so that others will not take advantage of different department.

Every department has their possibilities to connect to a Transfer folder, which is used to be use by the workers which work in office within related department. The typical corporate Local Area Network (LAN) or Wide Area Network (WAN) is an example of a private network. This is not used in the Company.

The line between a private and public network has always been drawn at the gateway router, where a company will erect a firewall to keep intruders from the public network out of their private network, or to keep their own internal users from perusing the public network.

Bechtel-Enka GP leased phone lines, however, can be expensive; they have to give mobile phones using intern Company or abroad as the company needs are. But, because a company has offices across the country, this cost can be prohibitive. So, there is a better solution. If

one of workers of a company doesn't happen to be near one of the corporate computers, he or she has to dial into a corporation's modem long-distance, which is an extremely expensive proposition.

Another hand, company must be about to use the virtual private network (VPN), a concept that blurs the line between a public and private network. VPNs allow workers to create a secure, private network over a public network such as the Internet.Some client and/or connecting networks may have been granted more access rights than is actually needed. They can be created using software, hardware, or a combination of the two that creates a secure link between peers over a public network.

This is done through encryption, authentication, packet tunneling, and firewalls. A policy enforced Network is a management architecture in which the creation and enforcement of Companies rules which is designed to bring structure and information's from the network to the places where they are stationed in a campus or distributed around on site, near Suhareka or around in Prizren. I have to mention that within policy group it may have a big point business rules which are concerned membership, traffic flow including data authentication, encryption…

And the members of this policy group are a part of Management domain and protect communications between trusted parties and firewalls access to communications that are not trusted domains in an information network.

Another word policy rules determine how the members and endpoint groups as a department of a policy group communicate by each other, also we must say that an e-mail exactly outlook which is used by office workers used to retrieve e-mail from remote server over an Internet connection.

2.2.1 Advantages of VPN

VPNs are more cost-effective for large companies as Bechtel – Enka GP is, and well within the reach of smaller ones.VPNs allow you to take advantage of business opportunities on the internet without increasing the risk to company assets. Virtual private networking also allows you to take advantage of the vast array of computing client platforms, such as laptops, Pocket PCs, smart phones, Tablet PCs, and other devices.

The list is limitless. Using VPN, you can use the Internet to communicate to any and every type of client, which opens up possibilities for your Users to work where they want to and optimize their performance and the performance of the Company. In this case Bechtel-Enka GP is connecting network in that which can be compromised if the client side is infected with a virus. If a virus or spyware infects a user's machine, there is chance that the password for the VPN connection might be leaked to an attacker. And this can cost much then user thinks.

In the case of an intranet or extranet VPN connection, if one network is infected by a virus or worm, that virus / worm can be spread quickly to other networks if anti-virus protection systems are ineffective.

So, Engineers which are supposed to work for IS&T department must control every server to get the job done. There is a server just for antivirus, which share to all computers in a Company. Another hand, if they just want to active an antivirus for every Computer in a camp there must be such lost time and cost also. So, there is a server for related job. I must say that for every mistake done or error in computer they just open a ticket and ask for help and there is shown a part of cloud computing, they share data between each other for a better communication.

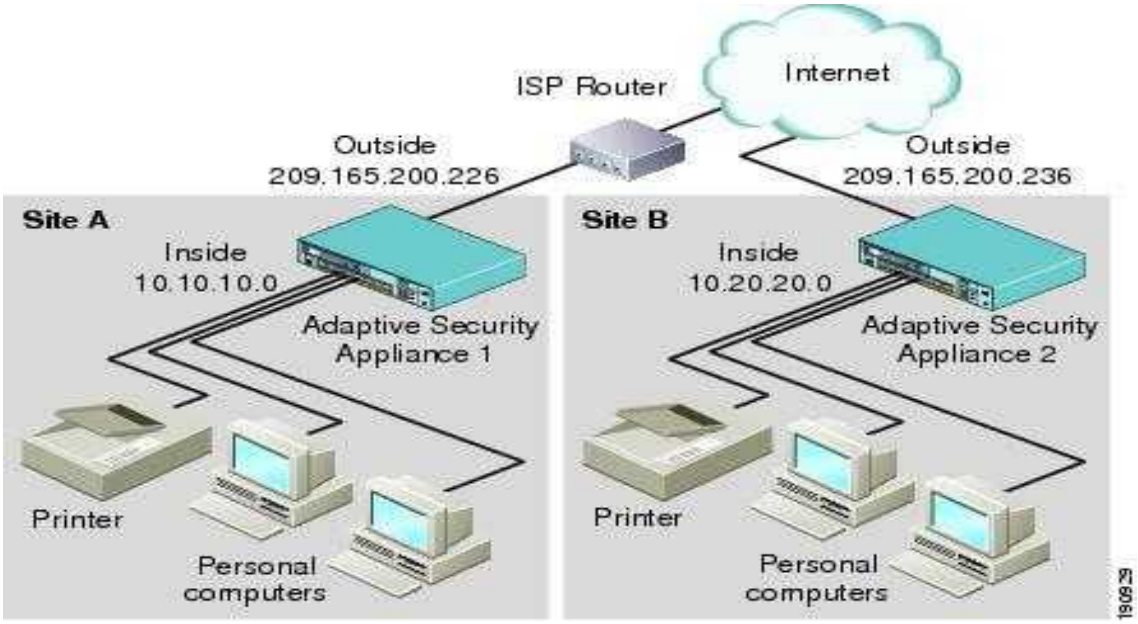

Figure 14: Advantages of VPN [14]

What more to say about VPN`s, a virtual private network (VPN) is a private communications network often used within a company, or by several companies or organizations, to communicate confidentially over a publicly accessible network. VPN message traffic can be carried over a public networking infrastructure (e.g. the Internet) on top of standard protocols, or over a service provider's private network with a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

2.2.1 Methods of using VPN

There are many different VPN technologies to choose from, and network operators need to put together a list of their requirements and pick a solution that meets these requirements. For a VPN user, such a list will typically include the following criteria.

In this Motorway Project is the way of departments which are responsible for a job which is related to department and also which is linked with the different department not as one but

with many. So, what I want to mention here is that every job done is equal to next job going to do. As it is described

• **VPN Service.**The VPN service must match the type of service required by the VPN user. Different VPN solutions offer either layer 2 or layer 3 connectivity between VPN sites. As described in section before, IS&T department this choice will depend on the type of traffic that will be sent between other offices in Suhareke, Kukes and Prishtina`s one, as well as the layer 2 and layer 3 protocols in use at each individual site.

•**Quality of Service.** The VPN user may require a certain quality of service (QoS) for the connections between VPN sites (for example, the VPN user may require a minimum guaranteed bandwidth). If this is the case Quality Department, the service provider backbone must support the provisioning of QoS-constrained tunnels, and the VPN solution must be able to make use of these tunnels. The Quality is asked from every department in every last days of month without any excuse of not doing the job as it is supposed to be.

• **Security.** If sensitive data is to be sent across the backbone between VPN sites, then the solution should support encryption, authentication and integrity checking of data in the VPN tunnels. In addition, it is a further advantage if the routing information distributed in the provider network is also protected, to prevent the VPN network topology from being exposed to prying eyes. Everything that is linked by the department of Security IS&T engineers are willing to provide the best solution for every little mistake or error.

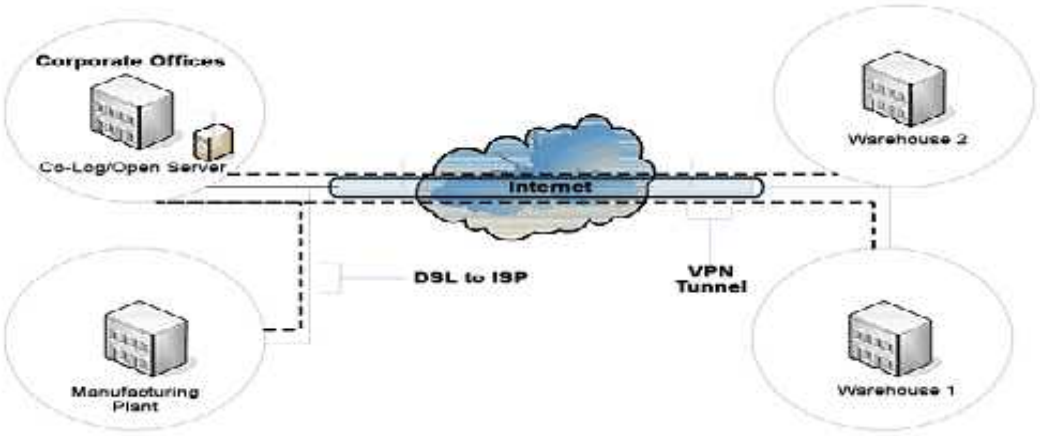

Figure 15: Security of VPN [15]

• **Capital Cost (to the VPN user).** The VPN user may require a solution that does not involve a costly replacement of their existing hardware. Therefore, any VPN solution offered by a service provider must not require expensive extra function to be added to the customer edge devices. Ideally, the solution will be fully workable with the VPN user's existing switches and routers.

• **Manageability.** The VPN user will want a solution that is simple to manage and which minimizes the migration costs. The configuration of the VPN solution should not be so complex that the network management personnel require extensive training. Neither should the solution require a significant overhaul of the VPN user's existing network architecture. Equally, the ongoing day-to-day management should not be too onerous – for example, it should be easy to add new sites to the VPN. But, we have to say that Business Management has such managed the job well and we suppose that he`s informed for any worm or virus in proper department linked by Subcontractor's and Procurement & Logistics.

• **Maturity.** The VPN user will want a solution that has widespread industry acceptance and deployment. Less mature solutions carry the risk that the technology may not yet be thoroughly tested, and the architectural and interoperability issues entirely overcome. There is also the danger that they may not be offered by an acceptable range of

provide and every engineer in a Project, limiting the VPN user's range of choice and ability to source alternative back-up solutions. At the same time, many workers and it may looking to differentiate their product or service offering by driving the establishment and deployment of new solutions.

2.2.3 Types of VPN

1. Secure VPN - It uses cryptographic tunneling protocols to provide the intended confidentiality, sender authentication, and message integrity to achieve privacy. When properly chosen, implemented, and used such techniques can provide secure communications overrun secured networks. The key feature is its ability to use public networks like the Internet rather than rely on private leased lines. Secure VPN protocols include the following:

• IPSec - IP security

• SSL - Secure Socket Layer

2. Trusted VPNs - They do not use cryptographic tunneling; instead rely on the security of a single provider's network to protect the traffic. Trusted VPN protocols include the following:

• L2VPN - Layer 2 VPN

• L3VPN - Layer 3 VPN

Since trusted VPNs work on private lines, we use circuit-switched networks instead of packet- switched network for the QoS reasons. In such a case Multi-protocol label switching (MPLS) becomes important. When customers rely on a provider for secure communication there is a Service Level Agreement (SLA) between the two, which not only decides on security terms but also QoS. Thus Resource Reservation Protocol (RSVP) comes into picture.

Secure VPNs use the tunneling mechanism to carry data on public internet lines. In tunneling data is transmitted through a public network in such a way that routing nodes in the public network are unaware that the transmission is part of a private network.

Encapsulating the private network data and protocol information within the public network protocol data so that the tunneled data is not available to anyone examining the transmitted data frames generally does tunneling. IPSec and SSL are commonly used in secure VPNs [12].

Trusted VPNs are provisioned and managed by Internet service providers by defining paths through their networks to ensure that customers' traffic is routed over a trusted path. A customer might choose a trusted VPN because there is no equipment to buy, it's completely managed by the service provider and thus requires no maintenance, and they often include service-level agreements. Typically, trusted VPNs are less expensive upfront but more expensive over time [5].

2.2.4 Layer 2/Layer 3

One major difference between types of VPN is the service that is provided to the VPN user. For example, an IP VPN service could be a Layer 2 solution (a "Layer 2 VPN" or "L2VPN"), providing customers with the likes of Ethernet, ATM/FR Virtual Circuits ("VC"s) or leased-lines, or could be a Layer 3 solution (L3VPN), providing customers with IPv4 or IPv6 connectivity between the VPN sites.

There are advantages and disadvantages for both of these, including the following.

1. Layer 2 solutions are in some ways more flexible – particularly in terms of the higher layer protocols used in the VPN. A layer 2 VPN may be transparent to higher layer protocols and so can carry IPv4 or IPv6, irrespective of the layer 3 protocol in the provider's IP network. This also means that some of these layer 2 solutions can also carry, for example, legacy SNA, NetBios and SPX/IPX traffic. However, the most common use for a VPN is to route IP traffic between the VPN sites, and so a layer 3 VPN is suitable for most purposes.
2. On the downside, some layer 2 solutions require that all the VPN sites run the same layer 2 protocol, which is not always possible.
3. Layer 3 VPNs can have advantages in terms of management. For example, in a managed layer 2 VPN, the customer is still responsible for all IP routing between

the customer sites, whereas in a managed layer 3 VPN, the service provider can take over this management burden.

3.0 Experimental design

VPNs enable you to set up secure communications between endpoints and are just one weapon in your security arsenal. Firewalls, an older and more established security technology, are common in almost every environment. A VPN should be integrated into your security policy and that means making sure your VPN and firewall play nicely with each other.

3.1Types of Firewalls

Three main types of firewalls are in common use today: packet filters, application gateways, and stateful inspection firewalls. They are described in the following sections with their characteristics and how the performance is showed in our Motorway Project.

3.2 Packet Filters

A packet filter is the simplest form of firewall. A packet filter firewall will compare any IP packet that attempts to traverse the firewall against its access control list (ACL). If the packet is allowed, it is sent through. If not, the packet filter can either silently drop the packet (DENY in ipchains speak) or send back an ICMP error response (REJECT).Packet filters only look at three things:

1. The source and destination IP addresses,
2. The source and destination ports, and
3. The protocol (UDP, TCP, and so on).

These tests are very fast because each packet contains all the data (in the packet headers) necessary to make its determination. Due to its simplicity and speed, a packet filter can be enabling your routers, eliminating the need for a dedicated firewall. One problem with packet filters is that they generally do not look deeply enough into the packet to have any idea what is actually being sent in the packet. Though you might have configured a packet filter to allow inbound access to port 25, the Simple Mail Transfer Protocol (SMTP) port, a packet filter would never know if some other protocol was used on that port. Another

problem with packet filters is that they are not effectively able to handle protocols that rely on multiple dynamic connections. The FTP protocol, for example, opens a command channel on which the various commands such as USER, RECV, and LIST are sent. For example, a user on one system might run his Secure Shell (SSH) daemon on that port, knowing that the packet filter would allow the traffic, and be able to SSH through the firewall against policy. Whenever data is transferred between the hosts, such as files or the LIST output, a separate connection is established. You would need to have an ACL that would allow these data connections through for FTP to work. However, packet filters do not read the FTP command channel to know when such an ACL should be permitted [9].

3.3 Application Gateways

An application gateway goes one step beyond a packet filter. Instead of simply checking the IP parameters, it actually looks at the application layer data. Individual application gateways are often called *proxies*, such as an SMTP proxy that understands the SMTP protocol.

The SMTP Protocol is used by office workers to have a better contact for a better job, whenever they are out of job, or missing in a work day, or even if they are in vacation time they would use SMTP of Company which is helpful in every kind of solution.

Here are some examples, in how to manipulate with SMTP. These proxies inspect the data that is being sent and verify that the specified protocol is being used correctly.

Let's say we were creating an SMTP application gateway. It would need to keep track of the state of the connection: Has the client sent a HELO/ELHO request? Has it sent a MAIL FROM before attempting to send a DATA request? As long as the protocol is obeyed, the proxy will shuttle the commands from the client to the server.

For example, you could tunnel any arbitrary protocol over SMTP: The client could send data as the DATA portion of the transaction, and the server could respond in the resulting error/success code message. The nature and ubiquity of the HTTP protocol makes it even

easier; SOAP and .NET are just two “accepted” examples of tunneling other protocols across HTTP. Http tunnel, available at www.httptunnel.com, is a good freeware tool capable of tunneling any protocol across HTTP.

The application gateway must understand the protocol and process both sides of the conversation. As such, it is a much more CPU-intensive process than a simple packet filter. However, this also lends it a greater element of security.

You will not be able to run the previously described SSH-over-port-25 trick when an application gateway is in the way because it will realize that SMTP is not in use. Additionally, because an application gateway understands the protocols in use, it is able to support tricky protocols such as FTP that create random data channels for each file transfer. As it reads the FTP command channel, it will see the data channel declaration and allow the specified port to traverse the firewall only until the data transfer is complete. Even application gateways can be fooled if you are crafty enough.

3.4 Firewalls Standards and Specifications

To define functional specifications and product standards for project's Internet firewalls. It is intended to satisfy the following set of business and technology objectives:

1. Provide global consistency to facilitate security and network management
2. Minimize complexity and administrative support
3. Safeguard the ability for future network upgrades as project's business and network technology evolves
4. Support requirements for client, supplier and partner connectivity

These standards apply to all interconnections within the project's network and between the project's network and the public Internet. For the purpose of this thesis, the project's network consists of a TCP/IP network: Under operational management of the project and Bounded by its Inter-NIC assigned address ranges.

The Internet is defined as any public shared IP network with unsecured connectivity to the Internet backbone. Any exception to these standards must be reviewed and approved by project's Information Systems and Technology (IS&T) Department. Stateful inspection firewalls are a middle ground between application gateways and packet filters. Rather than truly reading the whole dialog between client and server, a stateful inspection firewall will read only the amount necessary to determine how it should behave. In Motorway project Bechtel-Enka GP, I mean the IS&T department`s engineers take the SMTP DATA command, for example. When this command is sent, the office worker which might be someone from any department will send the data (the text of the email) ending with a line containing a single ".".

The server then responds with a success or error code. An application gateway will need to be reading all the data that is sent and looking for the "." and error code. A stateful inspection firewall, however, will realize that the engineer or any worker of office is sending data until the server responds.

Thus, it will simply forward the worker's packets without inspection until the server responds. Simply put, a stateful inspection firewall understands the manner in which stateful protocols must conduct themselves and manages that traffic accordingly within the confines of its rule base. By not reading all the data sent, a stateful inspection firewall achieves a significant performance gain over an application gateway while maintaining the higher level of security and protocol support. Our VPN traffic, however, will be encrypted end to end. As such, there will be very little that a stateful inspection firewall will need to look at in our VPN DataStream-it can't inspect the actual data anyway.

Because of this, there is no functional difference between a stateful inspection firewall and an application gateway for our VPN traffic. There is, however, a solid performance boost from using a stateful inspection firewall. Because our VPN is already introducing latency due to the overhead of encryption, the more performance you can get with your firewall, the better for you as a worker and for Project as help.

The firewall configuration standards consist of three sections:

- ✓ **Internet gateway design —** conceptual design for a typical project site
- ✓ **Firewall rules —** standard firewall rules to permit / deny specific network Protocols
- ✓ **Firewall product standards —** recommended hardware and software.

The general design for project's internet gateway consists of a hardware firewall (Checkpoint) behind internet connection Kujtesa Modem the traffic between the internet and the project's WAN, in addition to simplify network routing and a Web sense Internet Monitoring, Filtering Server.

WAN acceleration, TCP/UDP port and protocol filtering, as well as Web-sense Server which is used for its audit of employees Internet usage and restrictive functions, it caches frequently used Internet pages and it is also a firewall application. Unless expressly approved by project IS&T department, the only internal devices allowed direct outbound official project SMTP email gateway. The firewall performs NAT on all traffic between the internal Project network and the Internet. No data packets with un-translated project internal source addresses (e.g. 10.a.x.y) are permitted beyond the LAN.

The firewall is considered a network device. As such, it supports a rule set that restricts access by network addresses and protocols. In general, the firewall and proxy server both are well suited to perform content inspection and filtering tasks such as antivirus, blocking of objectionable websites. Here are some of firewall rules which help to be the work possible in different ways.

All access to the diagnostic ports of all devices will be strictly controlled and only authorized on as required basis, authorization being given by the IS&T manager. A tunnel is a means of forwarding data across a network from one node to another, as if the two nodes were directly connected. This is achieved by encapsulating the data – an extra header is

added to data sent by the transmitting end of the tunnel, and intermediate nodes based on and this outer header forward the data without looking at the contents of the original packet.

This is illustrated in the diagram below, which shows data going from A to B being sent through a tunnel between X and Z. The intermediate tunnel node, node Y, does not need to be aware of the final destination, B, but just forwards the data along the tunnel to Z.
(In this scenario, the tunnel knows X as the ingress and Z as the egress. just need to be able to forward tunneled data. This is important as it reduces the networker sources consumed by the VPN and the amount of configuration required to set it up.

In addition, by sending data between VPN sites using tunnels, it is possible to maintain separation of data between different VPNs, and to prevent data from a VPN being leaked into the provider network or global internet. It also means that the addresses of devices within the VPN sites are hidden in the data transported over the tunnel, so they do not need to be changed to allow them to communicate over the Internet.
The firewall standards are required as it is:

Ongoing standard hardware/software selection is addressed as part of the Project Enterprise Technical Infrastructure Committee standards review process. In that process, standards for hardware and software are defined and decided on, then listed in the standards database.

There are a number of protocols that may be used to establish these tunnels, and the properties of the tunnel have a significant effect on the overall properties of the VPN using that tunnel. However, many of the VPN solutions that we will describe do not rely on a particular tunneling technology and will work with one of several types.

For this reason, I do not cover the details of the tunnels when describing the different VPN solutions (except where necessary),as I described in before chapters the main properties of tunnels as supposed to consider are security and scalability.

A VPN customer whose data is being tunneled across a public network will want to know if that data is secure. As Camp needs are corporate VPN! So it is worth bearing in mind that the security of the tunnel is important for maintaining the privacy of VPN data - if the tunnel is not secure, it may be necessary for the Project to encrypt any sensitive data that is sent over the VPN.

The main issue with scalability is in the number of tunnels that may be required across the provider backbone, and the amount of network resource that the tunnels consume. In particular, it is a major advantage if the tunneling protocol allows multiplexing – in other words, if multiple data streams can be forwarded over the tunnel and then separated at the tunnel endpoint without requiring extra state in intermediate devices.

When multiplexing is possible, the provider network need only maintain a single mesh of tunnels between PE routers, which can be used by all VPNs. If multiplexing is not possible, then a separate mesh of tunnels is required for each VPN.

3.5 Cloud Computing

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud.

When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public.

Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. People can be users or providers of SaaS, or users or providers of Utility Computing. We focus on SaaS Providers (Cloud Users) and Cloud Providers, which have received less attention than SaaS Users [5].

From a hardware point of view, three aspects are new in Cloud Computing.

1. The illusion of infinite computing resources available on demand, thereby eliminating the need for Cloud Computing users to plan far ahead for provisioning.
2. The elimination of an up-front commitment by Cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.
3. The ability to pay for use of computing resources on a short-term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

We argue that the construction and operation of extremely large-scale, commodity-computer datacenters at lowcost locations was the key necessary enabler of Cloud Computing, for they uncovered the factors of 5 to 7 decrease in cost of electricity, network bandwidth, operations, software, and hardware available at these very large economies

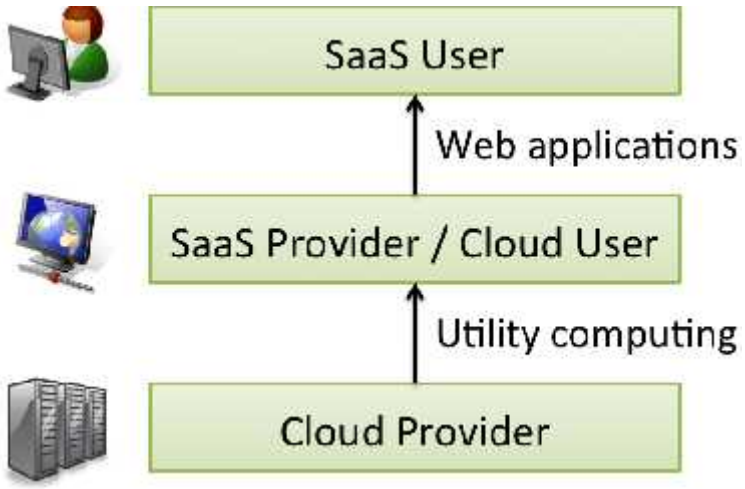

Figure 16: Quick Preview of Top 10 Obstacles to and Opportunities for Growth of Cloud Computing [16]

- ✓ Availability of Service Use Multiple Cloud Providers; Use Elasticity to Prevent DDOS

- ✓ Data Lock-In Standardize APIs; Compatible SW to enable Surge Computing
- ✓ Data Confidentiality and Auditability Deploy Encryption, VLANs, Firewalls; Geographical Data Storage
- ✓ Data Transfer Bottlenecks FedExing Disks; Data Backup/Archival; Higher BW Switches
- ✓ Performance Unpredictability Improved VM Support; Flash Memory; Gang Schedule VMs
- ✓ Scalable Storage Invent Scalable Store
- ✓ Bugs in Large Distributed Systems Invent Debugger that relies on Distributed VMs
- ✓ Scaling Quickly Invent Auto-Scaler that relies on ML; Snapshots for Conservation
- ✓ Reputation Fate Sharing Offer reputation-guarding services like those for email
- ✓ Software Licensing Pay-for-use licenses; Bulk use sales

3.6 Cloud Computing in Bechtel-Enka GP

Figure 17: Cloud computing sample picture [17]

Everyone has an opinion on what is cloud computing. It can be the ability to rent a server or a thousand servers and run a geophysical modeling application on the most powerful systems available anywhere. It can be the ability to rent a virtual server, load software on it, turn it on and off at will, or clone it ten times to meet a sudden workload demand.

It can be storing and securing immense amounts of data that is accessible only by authorized applications and users. This is what Bechtel-Enka GP support for their job, it can be supported by a cloud provider that sets up a platform that includes the OS, Apache, a MySQL™ database, Perl, Python, and PHP with the ability to scale automatically in response to changing workloads It can be using a storage cloud to hold application, business, and personal data which all are directly performed by IS&T department.

And it can be the ability to use a handful of Web services to integrate photos, maps, and GPS information which help engineers and designers to perform the job and in a way that are supposed.

Bechtel-Enka GP exactly the survey department uses the GPS information about the workers which are working on site and data which they are supposed to create including every description which could be accessed on that what they need just within `zero target` and safety rules.

Cloud computing can be the ability to use applications on the Internet that store and protect data while providing a service — anything including email, sales force automation and tax preparation. Like every Company in this century Bechtel-Enka GP uses the outlook to provide better job with no time lost.

To the extent that cloud computing helps to increase the velocity at which applications are deployed, helping to increase the pace of innovation, cloud computing may yet take forms that we still cannot imagine today. What remains constant, however, is that we use an experienced provider of server, storage, networking, and software technology that is ready to support cloud computing.

We believe that cloud computing is the next generation of network computing. So, we can say that this project can`t be as fast as it is done without communicating in this kind of work, we must be grateful on that what staff worker do with their knowledge’s and sharing ability with honor for a better carrier and good perspective in near future.

3.7 Types of Cloud Computing

Companies may make a number of considerations with regard to which cloud computing model they choose to employ, and they might use more than one model to solve different problems. An application needed on a temporary basis might be best suited for deployment in a public cloud because it helps to avoid the need to purchase additional equipment to solve a temporary need. Likewise, a permanent application, or one that has specific requirements on quality of service or location of data, might best be deployed in a private or hybrid cloud.

- Public clouds

Third parties run public clouds, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks (Figure 15).

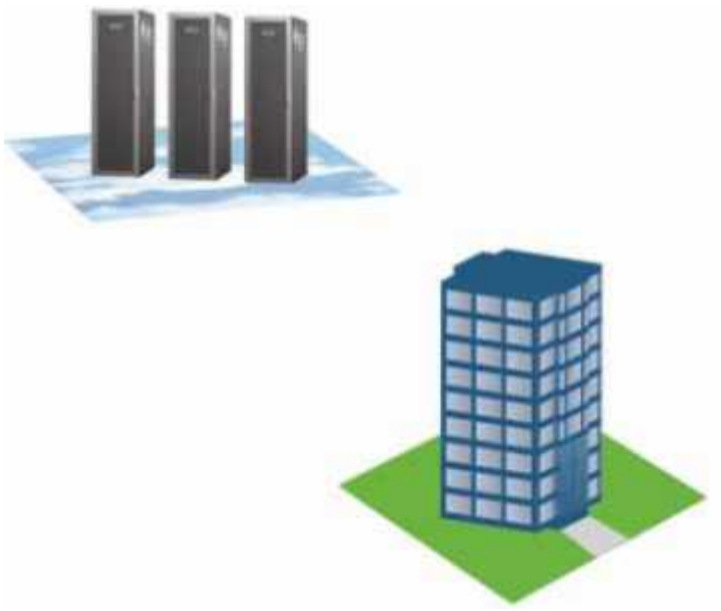

Figure 18: A public cloud [18]

Public clouds are most often hosted away from customer premises; this is an example of Suhareke Camp and Zhur Camp. In other words, they provide a way to reduce

customer risk and cost by providing a flexible, even temporary extension to enterprise infrastructure.

If a public cloud is implemented with performance, security, and data locality in mind, the existence of other applications running in the cloud should be transparent to cloud architects, designers, engineers and end users.

Indeed, one of the benefits of public clouds is that they can be much larger than a company's private cloud might be, offering the ability to scale up and down on demand, and shifting infrastructure risks from the enterprise to the cloud provider, if even just temporarily.

Portions of a public cloud can be carved out for the exclusive use of a single client, creating a virtual private datacenter. Rather than being limited to deploying virtual machine images in a public cloud, a virtual private datacenter gives engineers that are supposed for the related departments and safety supervisors and all the workers of that department greater visibility into its infrastructure.

Now departments within the whole Project engineers can manipulate not just virtual machine images, but also servers, storage systems, network devices, and network topology. Creating a virtual private datacenter with all components located in the same facility helps to lessen the issue of data locality because bandwidth is abundant and typically free when connecting resources within the same facility. *A public cloud provides services to multiple customers, and is typically deployed at a collocation facility.*

- Private clouds

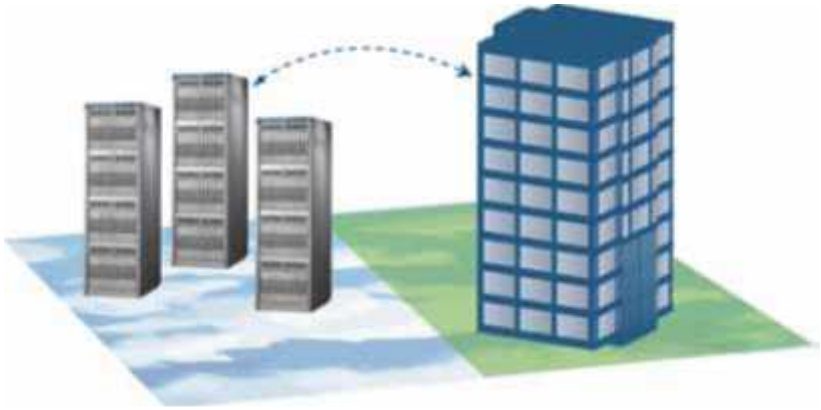

Figure 19: Private clouds [19]

Private clouds are built for the exclusive use of one client, this may be an example of Prishtina Office and Camp Zhur which providing the utmost control over data, security, and quality of service regarding by Project Control Department –Project Venture in this case owns the infrastructure and has control over how applications are deployed on it.

Private clouds may be deployed in an enterprise datacenter, and they also may be deployed at a collocation facility.

Private clouds can be built and managed by a company's own IT organization or by a cloud provider. In this "hosted private" model, another words whole Project Venture such as this Motorway Project an install, configure, and operate the infrastructure to support a private cloud within a company's enterprise datacenter.

Which with the all permissions we can say that they are doing it in a perfect way. This model gives companies a high level of control over the use of cloud resources while bringing in the expertise needed to establish and operate the environment. All documents, airfreights, Ministry Works, relations with all companies that are not near Camp and everything that must be done by Customs.

- Hybrid clouds

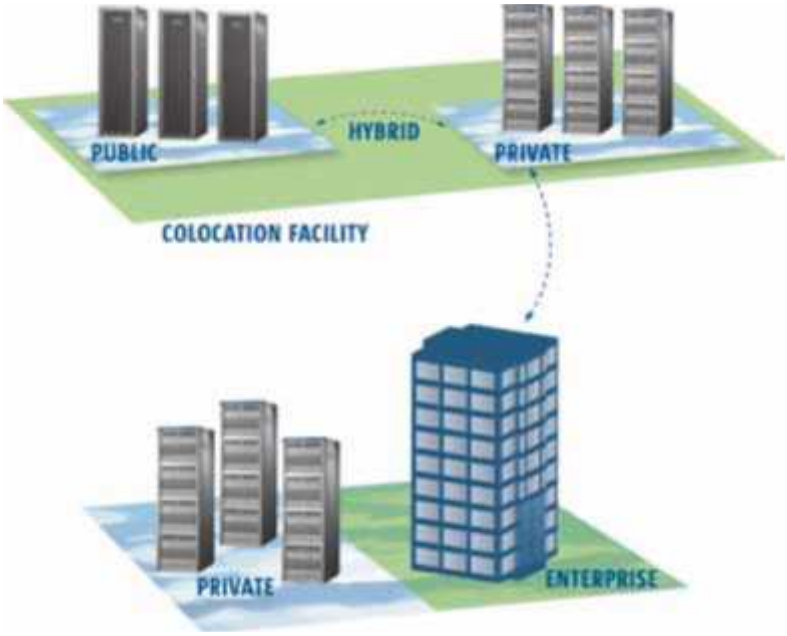

Figure 20: Hybrid clouds [20]

As it is described on figure Hybrid clouds combine both public and private cloud models. They can help to provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations. This is most often seen with the use of storage clouds to support Web 2.0 applications.

A hybrid cloud also can be used to handle planned workload spikes. Sometimes called "surge computing," a public cloud can be used to perform periodic tasks that can be deployed easily on a public cloud. This is a well example of Kukes Office by the Porject of Motorway 0f Albania and Zhur Camp.

Hybrid clouds introduce the complexity of determining how to distribute applications across both a public and private cloud. Among the issues that need to be considered is the relationship between data and processing resources. If the data is small, or the application is stateless, a hybrid cloud can be much more successful than if large amounts of data must be transferred into a public cloud for a small amount of processing.

So Cloud computing is the most popular notion in IT today; even an academic report from UC Berkeley says "Cloud Computing is likely to have the same impact on software that

foundries have had on the hardware industry." They go on to recommend that "developers would be wise to design their next generation of systems to be deployed into Cloud Computing".
While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud computing is here to stay.

Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud. Cloud fears largely system from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing third-party data storage and processing needs.
In our vision, we propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques. These measures should alleviate much of today's fear of cloud computing, and, we believe, have the potential to provide demonstrable business intelligence advantages to cloud participation.

Bechtel-Enka GP`s vision also relates to likely problems and abuses arising from a greater reliance on cloud computing, and how to maintain security in the face of such attacks. Namely, the new threats require new constructions to maintain and improve security.
Among these are tools to control and understand privacy leaks, perform authentication, and guarantee availability in the face of cloud denial-of-service attacks.

3.8 Database management systems

Database management systems have adapted to run in cloud environments by horizontally scaling database servers and partitioning tables across them. This technique, known as sharing, allows multiple instances of database software - often MySQL software to scale performance in a cloud environment.

Rather than accessing a single, central database, applications now access one of many database instances depending on which shard contains the desired data

Cloud Computing

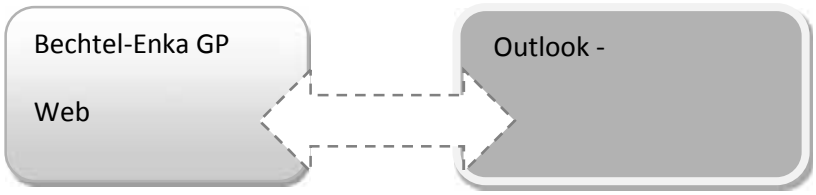

Figure 21: Cloud computing sample picture [21]

The overriding objective of good application architectures, however, has not changed at all: it is to support the same characteristics that have always been important:

1. *Scalability*-

This characteristic is just as important as it has ever been. Applications designed for cloud computing need to scale with workload demands so that performance and compliance with service levels remain on target. In order to achieve this, applications and their data must be loosely coupled to maximize scalability. The term *elastic* often applies to scaling cloud applications because they must not only be ready to scale up, but also scale down as workload diminish in order to not run up the cost of deploying in the cloud.

2. *Availability*-

Whether the application serves the users of social networking sites, or it manages the supply chain for a large manufacturing company, users of Internet applications expect them to be up and running every minute of every day. In this Motorway Project has been an industry leader in this area establishing early on its Project certification program that helped Engineers and Designers' to certify that its applications and services would stand up to required availability levels.

3. *Reliability*-

The emphasis on reliability has shifted over time. When large applications meant large symmetric multiprocessing systems, reliability meant that system components rarely fail and can be replaced without disruption when they do. Today, reliability means that applications do not fail and most importantly they do not lose data. The way that architecture addresses this characteristic today is to design applications so that they continue to operate and their data remains intact despite the failure of one or more of the servers or virtual machines onto which they are decomposed. Where we once worried about the failure of individual server components, now we build applications so that entire servers can fail and not cause disruption.

4. *Security-*

Applications need to provide access only to authorized, authenticated users, and those users need to be able to trust that their data is secure. This is true whether the application helps individual users on the Internet prepare their tax returns, or whether the application exchanges confidential information between a company and its suppliers. It is such a systemic property that we no longer call it out as its own principle — security must be integrated into every aspect of an application and its deployment and operational architecture and processes [7].

5. *Flexibility and agility–*

These characteristics are increasingly important, as business organizations find themselves having to adapt even more rapidly to changing business conditions by increasing the velocity at which applications are delivered into customer hands. Cloud computing stresses getting applications to market very quickly by using the most appropriate building blocks to get the job done rapidly.

6. *Serviceability-*

Once an application is deployed, it needs to be maintained. In the past this meant using servers that could be repaired without, or with minimal, downtime. Today it means that an application's underlying infrastructure components can be updated or even replaced without disrupting its characteristics including availability and security [24].

7. *Efficiency*

This is the new characteristic on the list, and it is perhaps one that most differentiates the cloud computing style from others. Efficiency is the point of cloud computing, and if an application can't be deployed in the cloud quickly and easily, while benefitting from the pay-by-the-sip model, it may not be a good candidate.

Enterprise resource planning applications, for example, may be best suited to vertically scaled systems and provided through SaaS in the near term. Applications that extract, manipulate, and present data derived from these systems, however, may be well suited to deployment in the cloud.

3.9 Installing Microsoft VPN

Click the Windows "Start" button and select "All Programs." Select "Administrative Tools" and choose "Routing and Remote Access."

Click the name of the server you want to configure and select "Configure and Enable Routing and Remote Access." Click "Next."

Select "Virtual private network (VPN server)" and click the "Next" button.

Ensure that the TCP/IP selection is made in the next window, and select "Yes, all of the available protocols are on this list." Click the "Next" button.

Select the Internet connection that is used to establish connectivity. This can be any one of the configured connections in the "Networking" section of the control panel.

Select the option that says "Automatically" assign for IP addresses. This enables the server to give IP addresses without needing to configure remote computers individually with static IP addresses.

Select "No, I don't want to set up this server to use RADIUS now." This window asks if you would like to configure multiple servers, but for this example, there is only one server to configure.

Click the "Next" button and then "Finish." This brings you back to the "Routing and Remote Access" console.

Right-click the "Ports" icon and select "Properties"

Select the "WAN Miniport (PPTP) device" installed on the server and click the "Configure" button. Enter the maximum number of remote port connections and click "OK." At this point, VPN services are installed and enabled on your server [18].

All that what I wrote till now, was described in proper way that I will explain with the figures down chapters?

3.10 Limitation of VPN

Despite their popularity, VPNs are not perfect and limitations exist as is true for any technology. The Project should consider issues like the below when deploying and using virtual private networks in their operations:

1. VPNs require detailed understanding of network security issues and careful installation / configuration to ensure sufficient protection on a public network like the Internet.
2. The reliability and performance of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.
3. Historically, VPN products and solutions from different vendors have not always been compatible due to issues with VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give as great a cost savings.

Virtual private network technology is based on the idea of tunneling. **VPN tunneling** involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.

For Internet-based VPNs, packets in one of several VPN protocols are encapsulated with Internet Protocol packets. VPN protocols also support authentication and encryption to keep the tunnels secure.

3.11 What we pretend to protect with VPN!

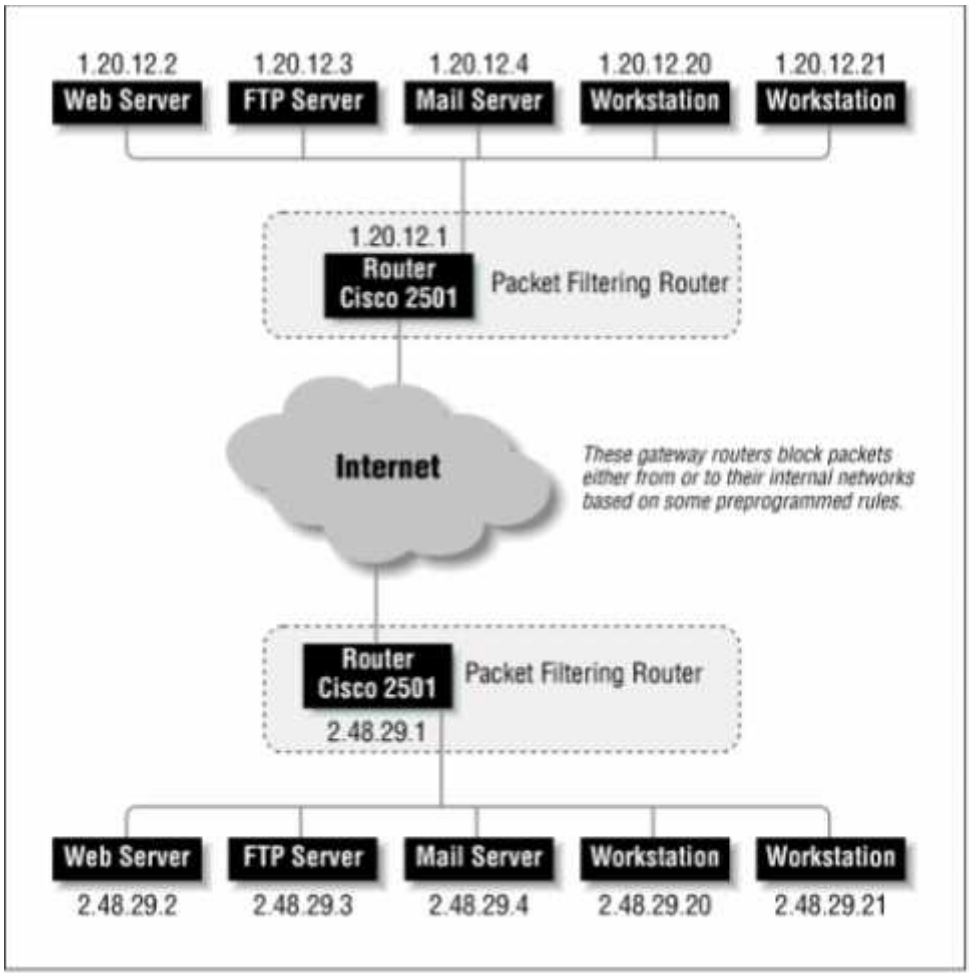

Figure 22: Firewall example [22]

Since almost all firewalling techniques are designed around a similar model, as we know Firewalls usually serve two main functions for a network administrator. The first is to control which machines an outsider can see and the services on those machines with which he can converse.

The second controls what machines on the Internet an internal user can see, as well as what services he can use. Firewall techniques are the first line of protection in the

fabric of a VPN, and they must be developed and tested before the benefits of the VPN can be fully harvested.

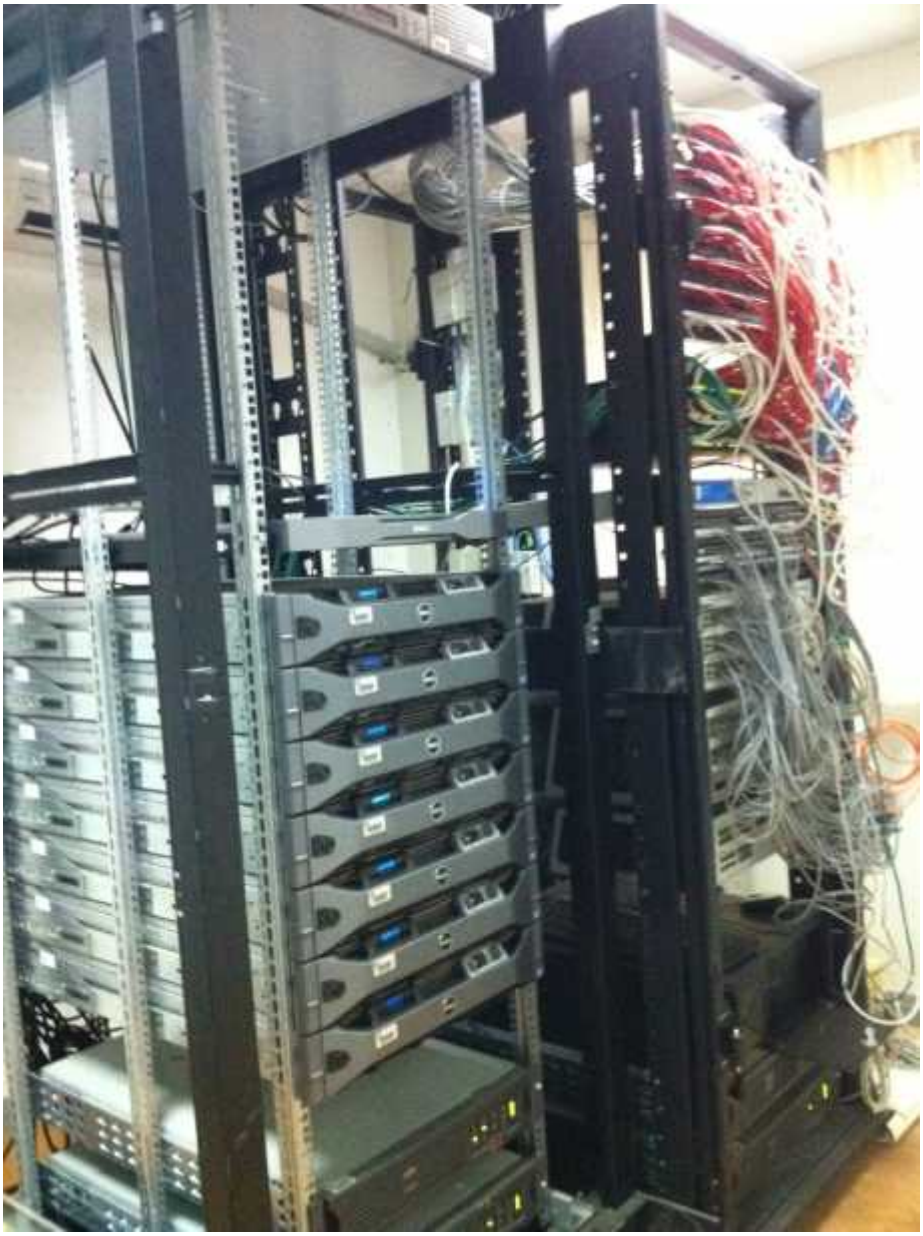

Figure 23: A picture of Server room in a Zhur Camp [23]

Even if the VPN software or hardware you deploy has built-in firewalling that seems to be everything you would ever need, chances are that you will need to follow some security guidelines on your network anyway, just to stay on the safe side. The importance of firewalling to a virtual private network is straightforward and to the point.

Since a VPN is an interconnection of two or more disconnected networks utilizing public resources (such as the Internet) for transit, it follows that these networks individually must be protected in and of themselves. Imagine each network that needs to be placed in a VPN as a separate bubble, with its own connections and users [9].

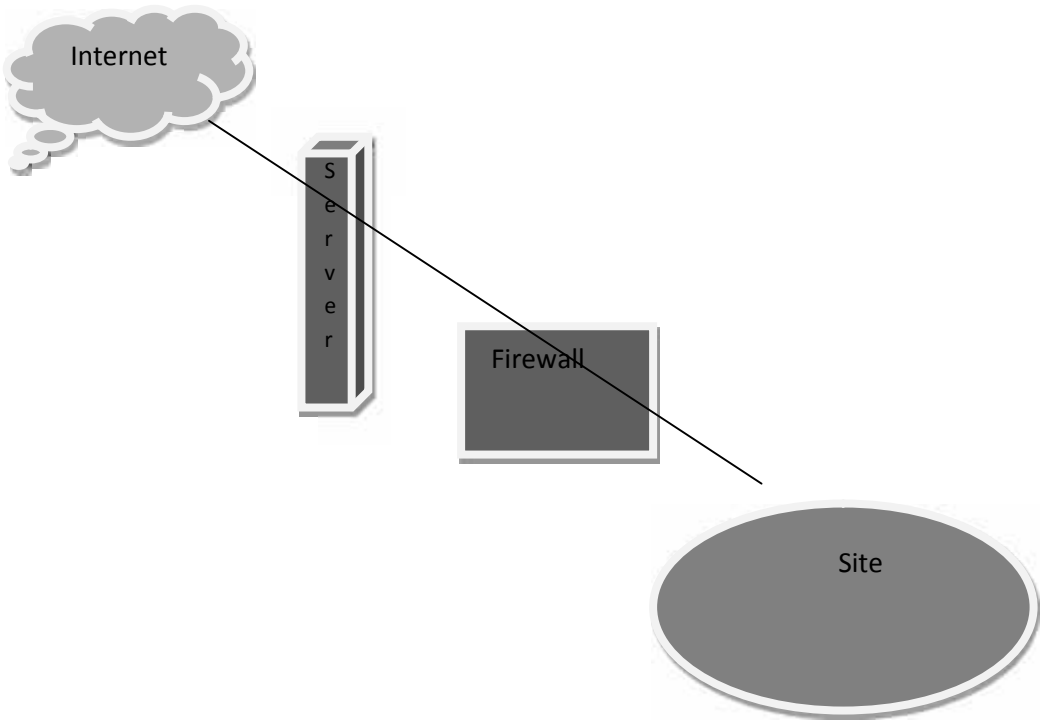

Figure 24: The VPN server in front of the firewall [24]

Because the firewall does not have the encryption keys for each VPN connection, it can filter only on the plaintext headers of the tunneled data. In other words, all tunneled data passes through the firewall. So, in this Motorway they used to provide just a Firewall

Server. This is not a security concern, however, because the VPN connection requires an authentication process that prevents unauthorized access beyond the VPN server.

Another configuration is when the VPN server computer is placed on the perimeter network between two firewalls. The Internet firewall, which is the firewall between the Internet and the VPN server, filters all Internet traffic from all Internet clients.

The intranet firewall, which is the firewall between the VPN server and the intranet, filters intranet traffic from VPN clients. Because the firewall does not have the encryption keys for each VPN connection, it can filter only on the plaintext headers of the tunneled data.

In other words, all tunneled data passes through the firewall. This is not a security concern, however, because the VPN connection requires an authentication process that prevents unauthorized access beyond the VPN server.

IPSec VPNs are the most widely deployed VPNs and are found in three main contexts:

1. Site-to-site IPSec VPNs –

   Tunnels are maintained by hardware devices to connect multiple users at remote branches to (one or more) central sites.

   Many of the same considerations required by private WANs need to be taken into account for IPSec VPN scenarios because they usually are deployed over the same Layer 2 WAN access media. IPSec VPNs also share some similar concerns with MPLS VPNs.

2. Teleworker IPSec VPNs-

   Tunnels are maintained by hardware devices to connect (typically) a single user at his or her residence to a central site.

   Solutions include these main benefits:

3. Increased productivity

   On average, employees spend 60 percent of their time or less at theirDesks, yet this are where the bulk of investment is made in providing access to corporate applications. Providing similar services at an employee’s residence, for a relatively minor investment, significantly can increase productivity gains.

4. Business resilience

   Employees can be displaced from their normal workplace by natural events (such as winter storms, hurricanes, or earthquakes), health alerts (such as SARS), man-made events (such as travel restrictions or traffic conditions), or simply family-related events, such as sick children or home repairs. These disruptions significantly can impact an organization's processes. Providing employees with central site–equivalent access to applications and services in geographically dispersed locations (such as home offices) creates a built-in back-up plan to keep business processes functioning in unforeseen circumstances.

5. Cost savings

   A traditional remote worker setup involves toll charges for dial-up and additional phone lines. Integrating services into a single, broadband-based connection can eliminate these charges while delivering superior overall connectivity performance.

6. Security

   Demands for access to enterprise applications outside the campus are stretching the limits of security policies. Teleworking over IPSec VPNs offers inherent security provided by encryption of all traffic, including data, voice, and video.

   Today enterprises need the flexibility of hiring skilled employees wherever the skills exist and need to integrate remote workers into geographically dispersed teams with access to equivalent corporate applications.

   Although QoS designs for IPSec V3PN teleworker scenarios share many of the same concerns ofsite-to- site V3PN scenarios, additional specific considerations relating to teleworker deployment models and broadband access technologies need to be taken into account.

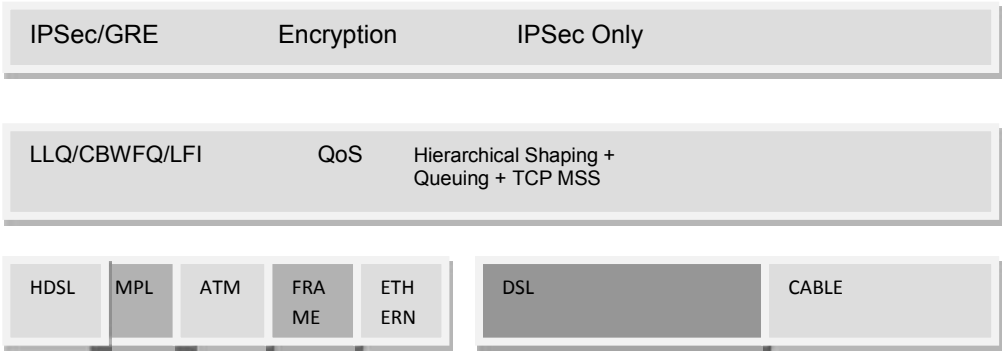

Figure 25: IPSec V3PN Site-to-Site and Teleworker Design Summary Comparison [25]

Site to site Teleworker

1. Remote-access client (mobility) IPSec VPNs-Tunnels is established by software to connect mobile users at airports, hotels, or similar places to a central site using WLAN hotspots, LAN ports, or modems.

   Enabling converged services, such as voice and video, on an IPSec VPN has been dubbed V3PN. V3PN is essentially the overlaying of QoS technologies over IPSec VPNs to provide the required service levels to voice and video applications. As such, V3PN solutions relate to only two of the three IPSec VPN design contexts: site-to-site VPNs and telecommuter VPNs. (Little, if any, QoS is available in remote-access client networks.)

   In this chapter discusses QoS design considerations and recommendations for both site-to-site and telecommuter V3PN solutions. These considerations include the following:
2. IPSec modes of operation
3. Bandwidth and delay increases because of encryption
4. IPSec and cRTP incompatibility -The significant increases in bandwidth required by IPSec encryption lead many administrators to consider the use of IP RTP header compression (cRTP) to offset these increases. Although developments are under

way to address these incompatibilities, at the time of this writing, cRTP cannot be utilized to achieve bandwidth savings in an IPSec VPN environment.

5. IP ToS byte preservation through IPSec encryption
   QoS and Anti-Replay interaction implications [6].

4. **Problem Statement**

What the entire project needs is to be secure in every part, in this case VPN has to be the point of security, which enables data to be transmitted without defects, where everyone is informed and has data in their hand in the right time.

Different cases may occur during using VPN, so every time you try to use VPN must be sure that at least you have these issues on:

There could be problem with the server you are trying to connect to, with the modem, with the IP, or it could be certificate problem etc. So, if all these things are solved then resources need to increase and the client has the project in time without any waiting that is cased from VPN, which could be unacceptable.

Well, during reading about VPN I didn’t find it hard to find data but I thought that to use information from Six Sigma training was helpful in some points.

5. Methodology

As it is bachelor thesis, it weren't supposed to have any research of thing that was happening in new technology and innovation. The focused part it was in searching for the points I pretend to have as a big picture. During the time I worked in Bechtel-Enka I searched for books which were related to Network, end exactly the chapters that have more common lessons with VPN, QoS , Security, Data clouding etc.

In this case I focused most of the time to find easier about VPN and other features.

So working in a big project wasn't so easy to have attention and understand all the work done there, so you have to go through days and months looking and have knowledge's about networking. So, the methodology I tried to use and I think it was helpful it was in that time I was working in Procurement department and be a buyer for the It department , so that part helped me to have much more time spent in having ideas and details in how they started the work within Security, QoS and new technology which were very useful.

Having such a big project in hand it means you have to have different and difficult works under your hand, so IS&T department have to have forecast plan, which exactly is a part of methodology of a department.

In a forecast plan are detailed plans without execution of any issues, so we must keep in our mind that a security testing is a strategic effort.

In this case if the forecast is done in any point they are ready to plan and continue to implement the other issues and strategies till the end of the project and so.

First of all I tried to spend more time with the IT managers which they supported me in this direction. The procedures were also a part of my thesis that I used to read and to see how they implement every step into a project.

So during that time I manage after work time to have more data about Security, Qos, Data clouding and every detail which was used by the project and implemented in different times.

According to the project requirements, network topology, system sesource, the apporiate and reliable service can be developed.

In other hand, searching about books, pdf files in internet was another part of methodology of my thesis. This is an aproach and I must achieve more than I used to believe. Actualy, all the searching part took more time as I thought it was supposed to spent. So, I considerated that the searching part has to be more valuable if I have in my thesis literature from different authors, diffferent researchments and everything that was shared in internet .

Also I have to mention that all this thesis is about how the VPN and other data was impelement in Bechtel-enka during the time I was working there, and examples in how Cisco or Miscrosft is impelementing it . This will be a part of lesson learnt that mean I deserve more than I pretend to have from this thesis.

In conclusion this methodology used in my thesis does not offer any new technology that is not known ,all is an hard work with some experience in networking and more reading articles, magazines , books related to network .

6. DISCUSSIONS AND CONCLUSION

The idea to create VPN is quite simple and I found it as `helpful` solution for every large company. It is a solution and chose problems between public and private networks. It allows you to create a secure, private network over a public network such as the Internet.
So, using related software, hardware or a combination of two both let us create a secure link between peers over a public network. Encryption, authentication, packet tunneling and firewalls do this all.
As a business grows, it might expand to multiple companies or offices across the country and around the world. To keep things running efficiently, the people working in those locations need a fast, secure and reliable way to share information across computer networks. In addition, traveling employees like construction people need an equally secure and reliable way to connect to their business's computer network from remote locations.

It is important to understand which features are supported and which features are not supported in the VPN 3.5 Client. For example, the Easy VPN Client supports 3DES, which is important, but it does not support DSS, Diffie-Hellman group 1 (DH1), and Authentication Header (AH). Also when I`m describing the way how to simplify VPN`s work so there is also important to understand the process of adding a connection to the VPN 3.5 Client, which was covered in detail with the figures before.

By truly understanding the process of adding a connection to the VPN 3.5 Client, you can then streamline the installation of the VPN Client, while ensuring that the ultimate control of your network remains where it should—in your trusty, capable hands! [21].
All this is described and analyzed in different ways, I used to read books which are related to the Network and Telecommunication, so I can say that it was not as easy as I see right now, to get information and read such pdf files on internet make me think that I`m going to continue my masters on those programs.

Another hand, starting from the day I started to work in a Motorway Project of Kosova which is the biggest one after what I see myself learning new things in different ways, it was a big opportunity to learn such things that I learned in my lessons but I didn`t practice before. So, this was a chance for me to have a work with network, procurement, logistics and so.

I was describing before that there in camp as a biggest station of a Project so the other stations were in Suhareka wish was 30 km far away from Prizren, then Kukes Office which was used to take data and other works which were usable also from the Project of Albania to our Motorway Project, and the last one the main office in Prishtina which all were linked and provided new technology which was used by the engineers and people with all prospective rules done.

VPN, Cloud computing and Data were used also by just Managers of different departments of the Project, the responsible people related by the departments as it was in Camp and also in area outside. The IS&T department as it was explaining before is the department which take the risk of every move into hard copies, whole the project to be controlled by the data clouding, and technologies is not such an easy work; responsibilities take hard work and nights without sleep. The cost took another important place, where there the budget exists.

So, being linked and have better relationships between departments also take courage and well experience engineers another case a small problem in computer may have be in contact to a huge problem which then it’s a cause to VPN into Project.

Our primary security suggestion is to make the VPN the only entry point to your network from the Internet. That is, make sure all of your systems are blocked or otherwise inaccessible from the Internet unless outside users connect to it via a VPN.

Moreover, why this thesis is important, meaningful, and useful?

I wanted to mention also as an example the way that a calling is done and what are the ways to get the information during the time of working. When calling into an ISP that supports PPTP, the ISP on their remote access switch does all of the VPN work for you. You just have to configure your client as if you're dialing directly into your RAS server; the ISP's switch will pass all the authentication information to that RAS server.

When dialing into an ISP that doesn't support PPTP, you'll need to initiate a PPP call to the ISP using the Dial-Up Networking dialog box. Once the call has been connected, leave your PPP session up, select the PPTP entry you made (in our case, it's called Central Office VPN), and click the Dial button [20].

This will initiate the PPTP call to the corporate RAS server over your PPP Internet connection. As we know in everything we wait to have problems so there are numerous points of failure with VPNs. This makes tracking down the cause of a problem more difficult than it might be for a normal WAN or remote access connection. Among the possible problems are connectivity problems, authentication errors, and routing problems.
I want to apply also that a well-designed VPN can greatly benefit a company. For example, it can:

· Improve security
· Reduce operational costs versus traditional WAN
· Reduce transit time and transportation costs for remote users
· Improve productivity
· Simplify network topology
· Provide global networking opportunities
· Provide telecommuter support
· Provide broadband networking compatibility
· Provide faster ROI (return on investment) than traditional WAN

What features are needed in a well-designed VPN? It should incorporate:

· Security
· Reliability
· Scalability
· Network management [10].

7. REFERENCES

[1] Rajiv Ramazwani, K. S. *Routing and wavelength Assisment in All Optical Networks*,http://sce.umkc.edu/, date: 10December 2011

[2] R. Clauberg, A. H. *A Scalable Modular Architecture for SDH/SONET Technology, date : 05 April 2011*

[3] VPN Fundamentals- Chapter 2 – Cisco Courses, Windows Server 2003 - [Ms Press] - Deploying VPN – Virtual, date: 01 December 2011

[4] Nayna Networks, S. J. *Optical Networking,RECENT DEVELOPING.* OHIO, November 2002, Singapor, 30 June 2011

[5] Komal Chandra Joshi ,Cloud Computing: Vol.2, Issue 3, May-June 2012-2013, date: lecturer of Shiriam Institute and Technology , date:20 December 2011

[6] Vpn_ebook.pdf, IPSecQoS.pdf, May2011, Sun_Cloud_Computing.pdf,date:

[7] 15 December 2011Jain, R. *IP Over SONET.* OHIO, date: 24 March 2012

[8] Bala Rajagopalan, D. P. *OPTICAL NETWORKING SOLUTIONS FOR NEXT-GENERATION INTERNET NETWORKS, 2005, India, 20 October 2011*

[9] Kulathumani Vinodkrishnan, Nikhil Chandhok, Arjan Durresi, Raj Jain. *Survivability in IP over WDM networks, 17 February 2012*

[10] http://www.iitk.ac.in/cc/vpn_update/sslvpn.htm, about SSLN- VPN, Indian Institute of Technology Kampur, read: 14 May 2012

[11] Srinivasan Seetharaman, R. J. *IP over All-Optical Networks – Issues, 10 September 2011*

[12] Amaury Jourdan, D. C. *The Perspective of Optical Packet, Germany, March 2001, 26 February 2012*

[13] Windows Server 2003 - [Ms Press] - Deploying VPN – Virtual. USA 2003, 07 July 2012

[14] Chris Metz. The Latest in Virtual Private Networks: Part II. IEEE Internet Computing, 10 March 2012

[15] Virtual Private Networks, Second Edition, Charlie Scott, Paul Wolfe , Mike Erwin, January 1999, 13 February 2012

[16] Understanding Cisco IOS IPSec Support – chapter 7, January 2012

[17] Cisco IOS Remote Access Using Cisco Easy VPN- chapter 9, date:16 December 2011

[18] BECHTOLSHEIM, A. Cloud Computing and Cloud Networking. talk at UC Berkeley, December 2008, 01 September 2011

[19] Introduction to cloud computing, first edition 2009, 10 October 2011

[20] Internetworking Technology Overview, June 1999-pdf, 26 September 2011

[21] Charlie Scott, Paul Wolfie, Mike Erwin , Virtual private Network, Second Edition, , January 1999, 30 October 2011