Rodoya Takele Degefa

VPN Scenarios, Configuration and Analysis

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor's Thesis

October 22, 2015

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Rodoya Takele Degefa VPN Scenarios, Configurations and Analysis 50 pages + 8 appendices 17 December 2010
Degree	Information Technology
Degree Programme	Bachelor of Engineering
Specialisation option	Security and Networking
Instructor(s)	Erik Pätynen

The goal of this thesis was to create a secure VPN tunnel and a VPN policy for a small LAN and suggest a secure, resilient and robust network setup insight in the vulnerabilities of security, In particular of VPN and provide recommendations to remove or mitigate these vulnerabilities. The thesis aimed not only to provide Site-to-site Connectivity but also to make LAN and its shared resources and services available to a remote worker or workers, offering an integrated, reliable, secured service.

To attain this goal, a network topology was built using a packet tracer and implemented in the school laboratory. During the laboratory work site to site, IPSec remote access and SSL VPN configuration were made to get the results. Cisco configuration professional software and command line interface were both used as a tool. The network connection was successful and secured from end to end for the remote office employees.

No company will be unaffected without the right security protocols. Lack of security policy, configuration and the weakness in technology were found to be the reasons behind system vulnerability. Companies that want to set a local area network with the benefits mentioned in this thesis and implement them in to their security policy will have a strong secured network. This security system is monitored, measured and found to be effective in protecting a company's network system from internal and external attacks and to protect it from loss of resources.

Keywords	VPN, security, IPSEC, tunnel, site-to-site, remote access VPN

Contents

Abbreviations

ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CCP	Cisco Configuration Professional
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality Integrity and Availability
DES	Data Encryption Standard
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSEC	Internet Security Protocol
ISAKMP	Internet Security Association Key Management Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
L2TP	Layer Two Tunnelling Protocol
LAN	Local Area Network
LNS	L2TP Network Server
MPLS	Multi Protocol Label Switching
OSI	Open Systems Interconnections
PAP	Password Authentication Protocol
PPP	Point to Point Protocol
PPTP	Point to Point Tunnelling Protocol
SA	Security Association
SAD	Security Association Database
SSL	Secure Sockets Layer
SSTP	Secure Socket Tunnelling Protocol
TCP	Transmission Control Protocol
VPN	Virtual Private Network

1 Introduction

Today's businesses provide employees with the opportunity to work from home or on the road. When a company allows their staff to gain access to the internal network, it is important that this is done safely. Many company employees who are often travelling, or who simply do not need to sit at a fixed place in an office to do their job need to have a secure access to the company network. When one works from outside the environment and needs information to work, it is important that he or she gets access from his or her location. Today, a broadband connection makes possible a quick way to send and retrieve information over the Internet. Just as there are thieves in the community, there are people on the Internet attempting to get access to other people's computers to steal information, or just to destroy it**.**

A common solution to enable users' get access to the internal resources of the company is to build a well-organized security system and protect its users. This allows users to access the internal resources in a secured manner. Companies spend large sums of money to have as fast, secure and reliable a connection as possible. Employees should be able to safely connect to their company network from outside the office. This includes where they want to work from home, on a business trip, sitting at a customer waiting place or other possible situations where they want to access available information on the internal network. To make this possible, it is necessary to use a medium to communicate.

The goal of this project was to create a secure VPN tunnel and policy for a small LAN. VPN is a virtual private network. The word virtual implies that there is no physical network infrastructure dedicated to the private network. The thesis aims not only provide Site-to-site connectivity, but also make the LAN and its shared resources and services available to a remote worker or workers, offering an integrated, reliable, secured service. It also suggests a secure, resilient and robust network setup insight in the vulnerabilities of security, in particular of VPN and provide recommendations to remove or mitigate these vulnerabilities

2 Security and VPN Overview

2.1 Security Overview

Most businesses in today's society believe that the Internet is an important part of their business and to compete with other companies, they must be connected to it. But there are big risks to connect a corporate network to the Internet. When a company connects its network to the Internet it allows not only employees to have access to it, but also makes it possible for outsider`s to access the company's private network. The need for verification of accessibility to computer traffic has thus driven the development of the control of computer communications. [11; 1]

A Common solution to most security threats is virtual Private Network (VPN). VPN allows a user to access the internal resources of the company from an external network such as the Internet. This allows users to access the internal resources in a secure manner. The VPN technology is then preferable to have as fast, secure and reliable a connection as possible. This thesis addresses various VPN technologies. I will describe the common VPN protocols such as MPLS, IPSec and PPTP, and how users authenticate in a safe and smooth manner. I will also explain methods that can be used to make users VPN connection secure. [12; 1]

When a company allows work outside the secured environment office there, arise some security risks, for example:

- When an employee is using a private computer in a network that more users has access.
- The computer can be stolen.
- An insecure home network where the computer is used usually with no or poor WLAN encryption
- Connecting computers may be unsecured with poor anti-virus and firewall rules.

There are several ways to give the user access to information on a corporate network. A prerequisite is that the user has an Internet connection. After this requirement is satisfied, then there are a number of methods to use depending on what you have for safety and what kind of internal resources, the user might access.

Some of the methods the user can use are:

• Establishing a File Transfer Protocol (FTP) server with the necessary information
•Connecting with a remote desktop and work directly to a computer within the company network.
• Adhere to the corporate network through a VPN tunnel.

FTP is used to transfer files between a client and a server. This might be a sufficient solution in some cases, depending on what the users will access in the local network and how high securities the user seeks. If users need to access shared folders, FTP can be a possible option. FTP cannot be in use in a case where the user needs to work directly in applications or other resources on the corporate network. [14]

The disadvantage of FTP over SSL is that it is expensive and that the safety is in many cases inadequate. It uses encryption of control and data connections either all at once or one by one. The negotiation of the connection is time-consuming and since it is done two times both for the data Connection and for the control connection, this makes it expensive if a user is to transfer a large number of small files. [14]

A password is used to send and receive files and transfer without encrypting it in FTP. What happens when a user, for example, wants to open a file on the terminal server and the graphics is sent to another user who thus is able to read and work with it? This is unlike other telecommuting solutions where the files are sent from a server to a client, often over the Internet. The file might become corrupted or stolen. Nowadays replacing FTP by SCP or secure copy can be optional since SCP is considered as easier than SFTP or FTP. [14]

A third way to allow users to work from home is to establish a VPN tunnel. In this case we can work from outside environment in the same way as we would in an office and it can be connected directly to the branch network. Implementing a VPN solution requires a VPN gateway, which is a device that helps authenticate users, encrypt outgoing traffic and decrypt incoming traffic. A VPN gateway can be used as a corporate firewall, a user-friendly; easy to administer and secure solution. This can be created with resources that we have in the school testing laboratory. [6]

2.1.1 CIA Model

CIA is a model which takes into account different controlling methods; it can be physical control, technically controlling or human action. The name CIA is formed by taking the first letter of Confidentiality, integrity and availability. Confidentiality, integrity and availability are used as a benchmark in security model. Confidentiality is a method of protecting data from those who do not have access it, whereas; integrity securely keeps the originality of the data. Sometimes unauthorized viewers do not have access for data because of security attacks, while availability makes sure that the data will be available for authorized viewers. [1]

The CIA method can be applied in different ways, which solely revolve around the three policies. Cryptography is one form of transferring data which controls access by encrypting and decrypting the information. [2] Data integrity can be protected with mechanisms such as digital signatures and hash algorithms. Redundant network architectures and systems hardware design help us insure the availability of data. The security of a company should be well coordinated taking all the three models into consideration. Taking one of the three models seriously and forgetting the other might cost companies a lot of loss [5].

2.1.2 VPN Models

VPN has two models commonly
The overlay model means that the operator provides a leased controlled router-to-router connection for the customer but it does not control the routing. Figure 1 below justifies how a service supplier provides a connection and overlay implemented. In overlay VPN model, the service provider provides the customer with a direct link to a different network. Overlay provides point-to-point-link or tunnel between the client networks and participates in all routed traffic. The traffic link can be implemented in the OSI-model at level of1, 2 or 3. [8; 7]

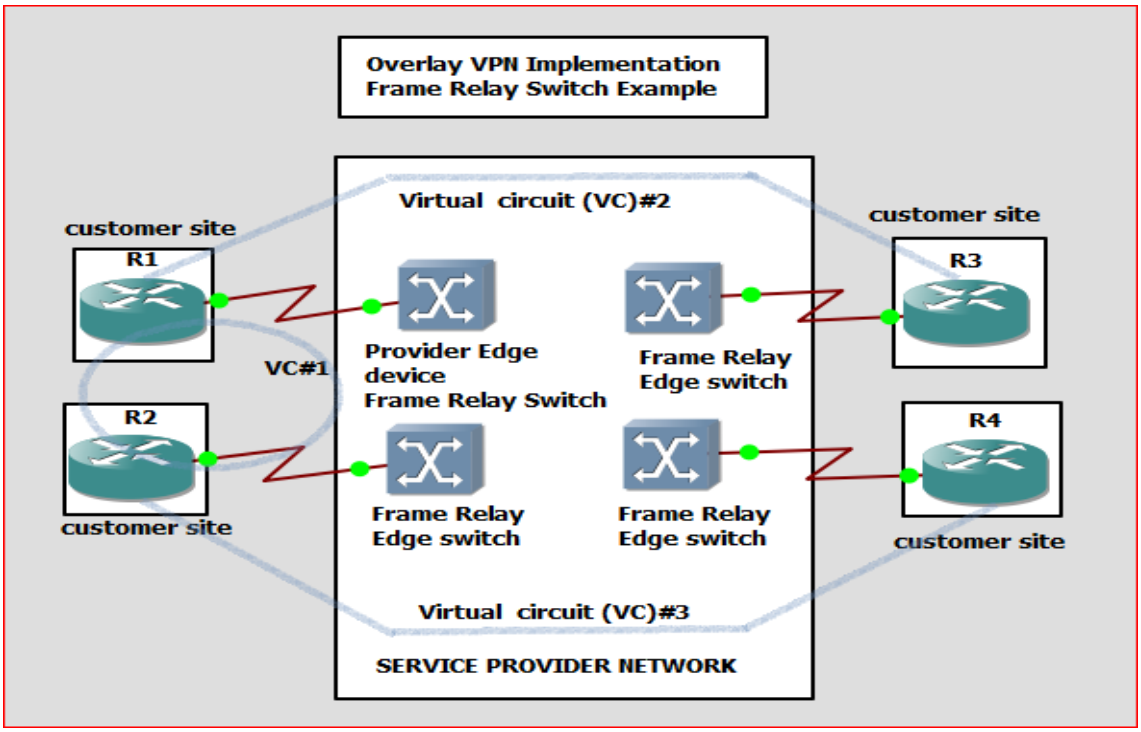


Figure 1.Overlay VPN

The peer-to-peer model means that the routing is controlled by the provider. These models allow separate private networks to merge, so that a single VPN network can belong to the same network alone. The VPN technology is a very important part of the modern network infrastructure, as companies, communities and networks are combined in such a way that the separate networks appear to be in the same internal network. [8]

In peer-to-peer VPN model, as shown in figure 2 the service provider participates in the customer traffic routing, whereas the service provider edge router connects to the neighbor customer edge router. The traditional peer-to-peer VPN-model problem is that configuration changes must be made in many places at the same time, if the client needs changes or wants to add or delete locations. Prior to the MPLS technology, the peer-to-peer model was hardly used, but VPN overlay model was the customer choice. [8]

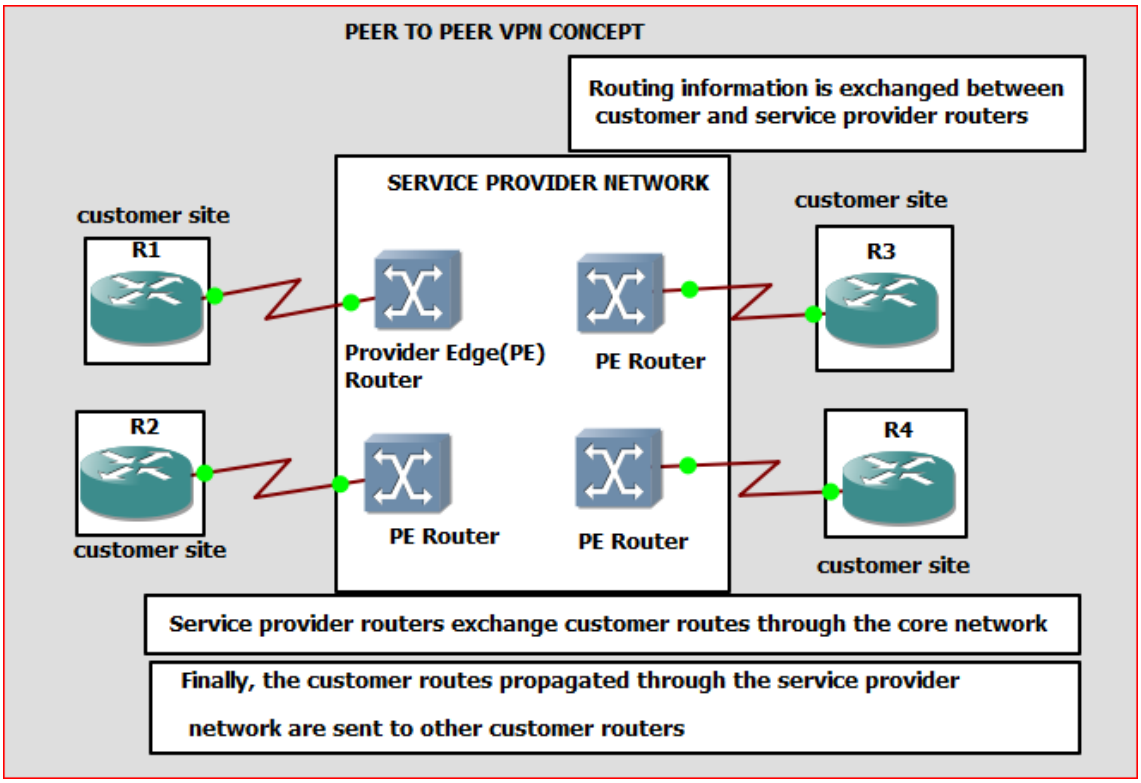


Figure 2.Peer-to-peer VPN

Overlay model can be as follows;

- Layer 2 examples are; Frame relay, ATM and MPLS Layer 3 examples PPTP L2TP and IPSec GRE
- Layer 4 example: SSL [3, 2]

Peer-to-peer model can be as follows;

- Dedicated router
- MPLS examples: BGP and VR
- Shared router [3, 2]

The basic motivation for using VPN is the need for secured communication. The first action when using VPN is to launch a VPN client on a computer and log in with the right credentials and exchange authentic keys with a server. Once both parties have verified each other's authenticity, all the data exchange will become encrypted and secured. [3]

2.2 VPN Tunnelling Protocols

Tunnelling means transferring data which uses a network framework to transfer data for a specific network over another network. Tunnelling encapsulates packets to be transmitted with an additional header and delivers it through a tunnel. Tunnelling mainly includes three steps: transferring data, encapsulation and decapsulation. Figure 3 shows the tunnelling process. Packets or payload will be encapsulated with an extra header in the beginning and they will be transferred through a tunnel and then decapsulated at the end of the tunnel. [10]

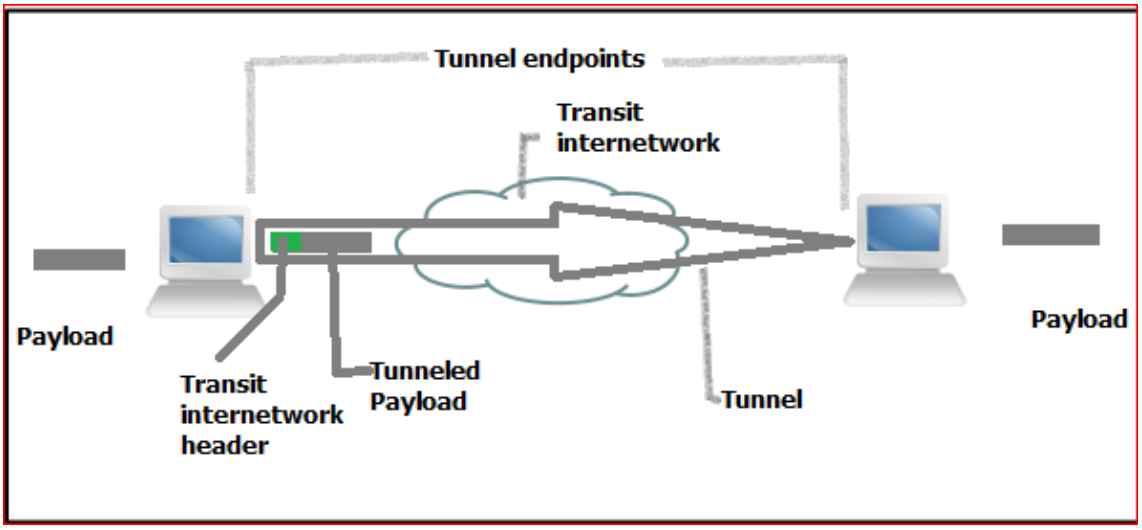


Figure 3.Tunneling

There are a number of different protocols to create safe tunnels between two network connections. One should carefully examine various options before implementing a VPN solution. Protocols are used to encapsulate and decapsulate the packets. The most widely used VPN protocols are such as L2TP, IPSec or PPTP. PPTP is a protocol used by VPN to encapsulate packets over a public switch network. [14, 9]

VPN Protocols

The following are very important VPN protocols that can be used to make a tunnel: PPTP, L2TP, GRE, IPSec, SSL and SSTP [14.10]

2.2.1 Point to Point Tunnelling Protocol (PPTP)

PPTP is a protocol that works in the second layer of the Open Systems Interconnection OSI model, called the data link layer. PPTP is an extension of the Point-to-Point Protocol (PPP). The protocol encapsulates PPP packets in the Internet Protocol (IP) packets. The reason for this to be done is that IP can be routed on the Internet. To explain this a little more closely, we should know how the PPP protocol operates. [14, 10]

PPP is a network protocol used to manage remote connections from clients to servers via a dialup or a serial point-to-point connection. A common use of PPP is when a user as a client establishes a connection to the Internet or Internet Service Provider (ISP) via a modem. The PPP protocol encapsulates an IP packet into PPP frames resembling the encapsulation of IP in Ethernet frames. Figure 4 shows how a PPTP packet looks like after encapsulation. These packages can then be used to create a point-to-point connection between the sending and the receiving computer. [10]

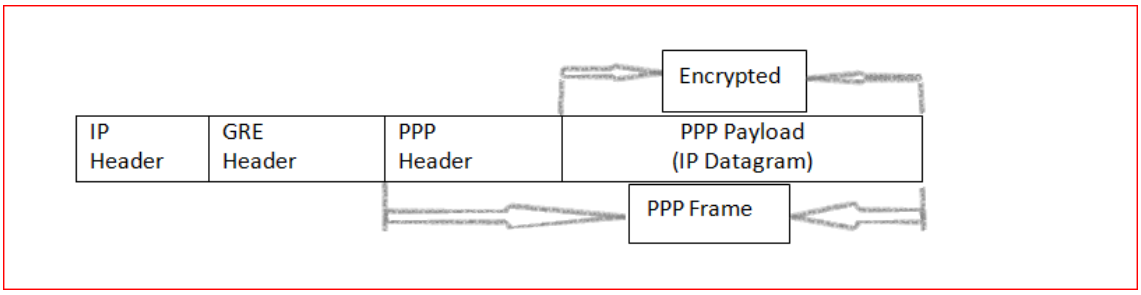


Figure 4.Structure of a PPTP packet

When a client connects to a PPTP server, the following occurs. The client has an IP packet that wants to send through a private network. This IP packet is encapsulated in a PPP framework to provide a point-to-point connection to the PPTP server. The PPP frame will be routed to the correct address on the internet as capsules of IP packets. Thus the packet leaving the client will look like Generic Routing Protocol (GRE) because of the tunneling protocol that packs the PPP packet in an IP packet. The PPP protocol is also responsible for the user authentication. [10]

Authentication methods that can be used are the Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) and or EAP Transport Layer Security, which EAP stands for Extensible Authentication Protocol (EAP-TLS).

Encryption in PPTP traffic is handled by Microsoft Point-to-Point Encryption (MPPE). The encryption algorithm which is used is RC4 and allows 40, 56 and 128 bit keys. [10]

2.2.2 Layer Two Tunnelling Protocol (L2TP)

PPP is the protocol used to encapsulate network layer protocols and send these over layer 2 point-to-point links. The user with a layer 2 connection to L2TP Access will have concentrator through one of the many technologies (such as modem connection via the telephone, ISDN or ADSL) and uses the PPP protocol over these media. In these cases, layer 2 connection and PPP protocol endpoint are the same, that is, in the LAC one. LAC is L2TP access concentrator. It is the initiator of the tunnel. [14, 10]

What L2TP does is to allow different endpoints for PPP and layer 2 connections. L2TP creates a layer 2 connection to an ISP connection point (LAC). This device uses PPP protocol. Figure 5 shows the structure of an L2TP packet. The access point then sends PPP packets to L2TP Network Server which lies on the other side of a packet-switched network such as the Internet or Frame Relay. The output of the solution is going to be to dial a local layer 2 connection. Then it sends these packets over a cheaper medium (e.g. the Internet) to the recipient's LNS device. This makes it considerably cheaper. LNS are L2TP Network Server that waits for new tunnel. [10]

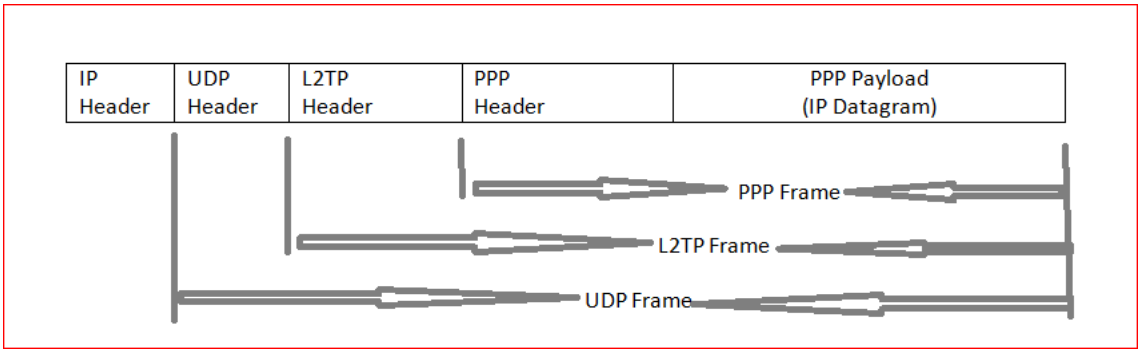


Figure 5.Structure of L2TP Packet

L2TP uses two different types of packets control or data packets. This is the easiest way to understand how these are used to describe in what way an L2TP connection is established and used once it is up. It starts with LAC unit it can be LAC client software or a LAC unit of an ISP. Then it sends a Start-Control-Connection-Request (SCCRQ) packages to LNS. This message contains host name, protocol version, tunnel ID, opportunities and Message Type Attribute Value Pair (AVP, a form of ID value). In addi-

tion to these information fields, there are additional fields that are optional. In this message the LNS responses with a Start-Control-Connection-Reply (SCCRP) message indicating the LNS has approved the parameters that were sent with the message SCCRQ [10]

When these two messages are sent LAC responses with a Start-Control-Connection Connected (SCCCN) message. When this is received, the L2TP tunnel will reside. A session can thus be drawn from both the LAC and LNS. The difference between these is that the LNS makes the call package to include more parameters than if the connection was established from the LAC. The second step in the establishment of a session is when the Incoming-Call-Reply (ICRP) and the corresponding Outgoing-Call-Reply (OCRP) package are sent in response to the requests. Both of these contain the same data, message type and the allocated session ID. After these messages, follow the Incoming-Call-Connected (ICCN) or equivalent Outgoing-Call-Connected (OCCN) packet that tells all parameters have been approved and that the session connection is now established. In these messages there are only three required fields message type, connection speed and inramnings type. [10]

The messages are all sent over a separate channel in the tunnel and used to set up and maintain the tunnel with the various sessions. For each L2TP tunnel there is a control channel and one or more sessions. Between the LAC and LNS more L2TP tunnels can be setup. Both the LAC and LNS must have a sequence number table where they keep track of which packets they receive and thus can see if any packages not arrive and then request a retransmission of the lost packet. [10]

2.2.3 Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation is a protocol that serves as a means of carrying traffic introduced by Cisco. It can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. GRE provides security with IPSec because it doesn’t have encryption. [14, 10]

As we can see from figure 6, when the router receives a packet for tunnelling, a routing decision will be made. It transfers it to the tunnel interface. The packet then will have a new IP and GRE header in the tunnel interface. Then the tunnelling interface encapsulates the packet. The second routing decision is to decide the departing interface based on the headers. Then finally the packet will be delivered to the relevant interface. [15]

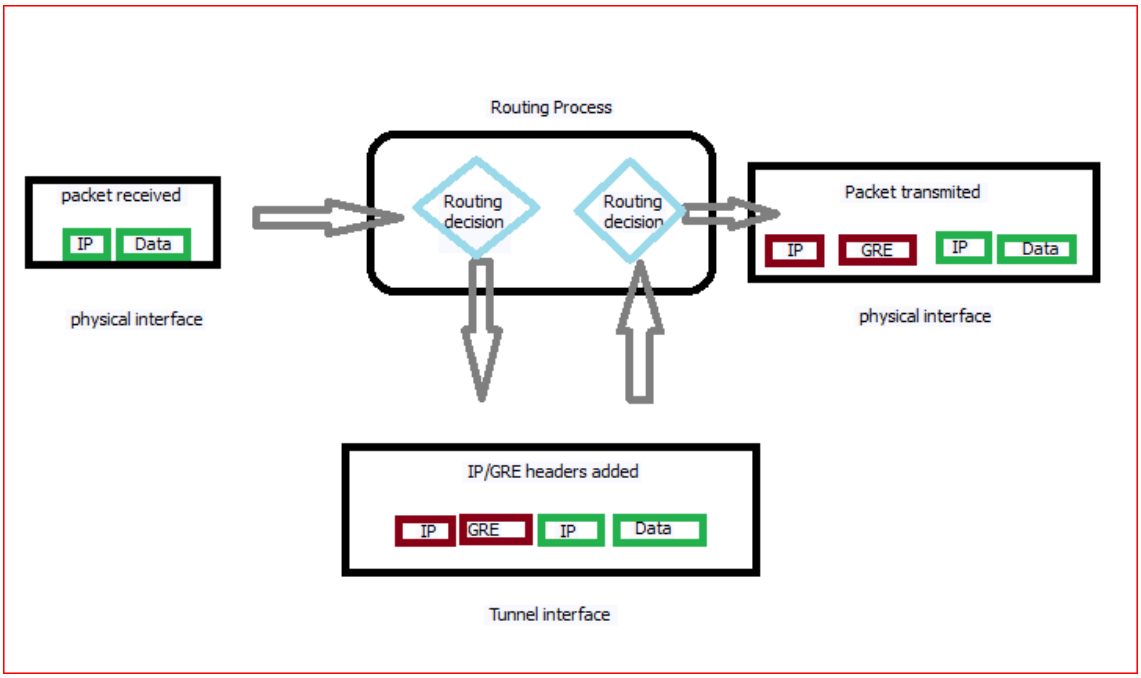


Figure 6.GRE encapsulation process

2.2.4 Internet Security Protocol (IPSec)

IP Security is a standard protocol that works with the IP protocol. It is built with different capabilities and protocols. A mass of RFCs defines how it should look like, how it needs to be implemented and how to use it. RFCs are a collection of documents discovered by different Internet engineering task forces or IETF and the internet community. RFCs clearly and in detail describe each protocol an IPSec uses and gives IPSec specifications. For example, IPSec, specified in RFC 4301, creates a boundary between protected and unprotected parts of the network. Packets passing through this border are treated differently. The packages, depending on the IPSec are configured, can pass unhindered, discarded or be treated with various services. A big advantage of IPSec is that it works at the network layer and works with both IPv4 and IPv6, which means that all existing applications can take advantage of IPSec without modification. [10]

Ipsec differs from traditional applications such as SSH, which operates at the application layer. IPSec has been developed to increase the security of IP communications. IPSec can be used in a point to point connection between two computers to make communications secure. IPSec can also provide secure communications between a connecting client and VPN server. IPSec is not a protocol but rather a protocol suite

that works with several protocols to perform their goals confidentiality, with integrity and authentication. [10.10]
The point I need to make clear is that, IPSec tunnels help only to secure unicast traffic but cannot be used to secure multicast or broadcast packets.

IPSec can be divided into two parts:

- Security Protocols are protocol that defines what information should be added to an IP packet to achieve precisely the confidentiality, integrity and authentication.
- Internet Key Exchange (IKE) is used to authenticate two devices. The devices exchange a secret session key to encrypt and decrypt data, and agree about which protocol to be used.[10]

2.2.5 Secure Sockets Layer (SSL)

Secure Sockets Layer protocol uses public and private keys to encrypt data and provide security. The HTTP protocol encrypts data and no software will be needed on the client side with since users will have a restricted access. It has a wide use in e-commerce and helps to securely make transactions online. [6; 7]
There are two phases in this protocol the first phase is exchanging key and the second phase is data transfer.

2.2.6 Secure Socket Tunnelling Protocol (SSTP)

A VPN protocol used to provide security for transmission of PPP and L2TP traffic. It allows traffic to pass through SSL 3.0 channels that allows transmission and data encryption. A TCP connection will be set up between the SSTP client and TCP port 443 on the SSTP server. Then the SSL session will be created and the client will receive a certificate from the server. The SSTP client generates the SSL session key and uses it to encrypt with the received certificate. The server after receiving the data decrypts SSL session key by using a private key of its own certificate. [10, 10]

2.3 Designing and Implementation of IPsec VPN

2.3.1 Security Protocols

Before we go deeper into this security protocol IPSec, we should first understand the two different modes that IPSec can run in namely tunnel mode and transport mode. To understand the differences between these, we should first know what an IP packet looks like. Figure 7 demonstrates an IP packets structure. [10, 17]

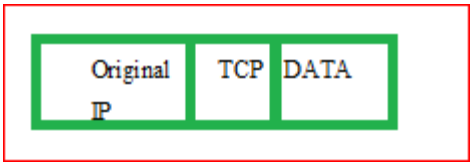


Figure 7.IP packets

When the transport mode is changed only the IP header is intact. This works when the receiver and transmitter are endpoints of the data exchange. To mention some examples, when two computers directly talk to each other, only one of these knows the other's address. Figure 8 shows what an IPSec packet looks like in the transport mode. [10, 17]

Figure 8.IPSec packets in transport model

In the tunnel mode the entire original packet will be encapsulated to form a new package and a new IP head. The tunnel mode is used in site-to-site solutions where two VPN gateways are talking directly to each other. These usually have static IP addresses. Below in Figure 9 we can see how IPSec packets will look like in a tunnel fashion. [10.17]

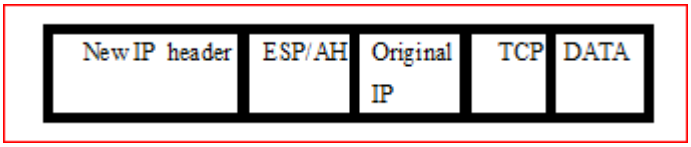


Figure 9.IPSec packets in a tunnel model

The main purpose of IPSec is to provide security to ordinary IP packets. Services such as IPSec use provide in order to make communication more secure include data integrity, authentication, and protection against replay attacks and data encryption. In order to offer these services IPSec uses two different protocols, namely the Authentication Header (AH) which is specified in RFC 4302 and Encapsulating Security Payload (ESP), specified in RFC 4303rd .AH provides integrity, authentication, and replay protection. ESP provides integrity, authentication, replay protection and reliability. [10, 17]

A major difference between AH and ESP is that AH can authenticate parts of the IP header while ESP can only authenticate the data. AH and ESP implements a variety of cryptographic algorithms to provide the various services. To ensure interoperability between different implementations of IPSec, RFC 4305 specifies a set of algorithms which are mandatory to implement. These algorithms are specified in the IPSec to leave room for future changes. [4]

Authentication Header (AH)

This IPSec protocol allows a digital signing of the IP header of each packet included in the IPSec transfer. The receiving computer verifies the signature of each packet through the use of a session key shared between the parties. If any piece of package has changed over shipment it will force the host computer to toss the package. By doing this, one can be sure that the IP packet is not changed during transport. It can also be sure that the sender is a legitimate user because only such a user can sign an IP packet with a valid session key. [10, 18]

The AH does not encrypt the data payload. By calculating a hash value of the entire IP packet and sending it to the receiver, integrity will be achieved and this calculation is called the Integrity Check Value (ICV). The transmitter calculates a hash value of package using a hash function or Message Authentication Code (MAC). To create integrity as the transmitter one uses the value in the hash function known only between the communicating parties. If the ICV field line with receiver estimates the packet it will be considered to be valid and received. [10, 18]

The hash functions used as IPSec for this purpose are usually the Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA1). It should be mentioned that recently successful attacks against these protocols have been made and a new stand-

ard is being developed. The safer of them is SHA-1. AH also provides protection against the playback of traffic via a simple counter in the AH header. This calculator gives each packet a sequence number and throws packets coming into the wrong order. [10, 18]

Encapsulating Security Payload (ESP)

ESP has the same features as the AH but also makes sure to encrypt the data load. ESP encrypts and authenticates the entire packet contents through the use of a shared session key. The receiving computer uses the same session key to decrypt the packet. The difference between AH and ESP is that ESP can encrypt the payload data. Encryption differs somewhat depending on whether one uses the tunnel or transport mode. During tunneling process it encrypts the original IP address while the new IP header is left untouched. But while the packet is in transport position it leaves the original IP address untouched and the rest of the packet will be encrypted. [10, 18]

The authentication process differs somewhat from the AH. The difference is that ESP is the hash sum not calculated on the whole package, but only on the part that has to do with ESP. ESP does not take the outermost IP header in to the calculation of the hash sum. In ESP, the same hash functions in the AH. The encryption algorithms used are typically Data Encryption Standard (DES) and Triple DES (TDES). [10.18]

2.3.2 Internet Key Exchange (IKE)

IKE is not really a protocol but a collection of protocol options, including the Internet Security Association and Key Management (ISAKMP). These protocols are used to create a secure channel between two communicating parties and to be able to communicate securely between two parties using IPSec, among other things, encryption and authentication. To be able to use encryption and authentication applies when the parties agree on the methods to be used. Before communication starts safely, they must exchange a secret session key to authenticate each other make sure the tunnel is safe. [10, 16]

All the parameters are negotiated between the two parties. IKE is saved in a Security Association (SA), which in turn are stored on each computer in SA Database (SAD).

Each package that is sent between the two devices communicating with the IPSec will have a value called the Security Parameter Index (SPI). [10, 16]

There are two types of security association (SA);

- IKE SA
- IPSec SA [10, 16]

2.4 Authentication of IPSec

2.4.1 Pre-shared Key

The Pre-shared key is the same key manually set to both parties involved in the communication. A hash value is calculated using information from the key and sent to the counterparty in communication. The other party performs the same calculation with his key and compares that value with the value given to it by the other party. After the comparison if the value is true, they share key and communication will continue. The disadvantage of this method is that since all users who connect using the same pre-shared key, someone, either of malice or accidentally, reveals the key. [10, 16]

The best way to avoid malicious attack during security negotiation is to encrypt the information before transmission by using a session key. If someone cracks the key of all computers in the company and VPN gateway reconfiguring can be a big job in a large organization. Therefore apply the solution best suited for smaller businesses. In order to make the password difficult to crack or guess the key should be complex. It is recommended to make the key at least 8 characters long and varied with lowercase letters, uppercase letters, numbers and special characters. [10, 16]

2.4.2 Certificate

The certificate is the most secure and scalable solution to manage the authentication of the IPSec. Certificate avoids password management contained in the pre-shared key variant. Instead, the user services are assigned a certificate by a so-called Certificate Authority (CA) that acts as a trusted third party. A certificate contains a name, a public key and a time when the certificate expires. A CA creates the certificate and signs it with its private key. The private key helps verify the signing access to the CA's public key, which only legitimate users have the access. [13]

3 Comparison of Different VPN Models

The suitable VPN solutions for a company can be selected through the following factors; the first can be based on the operating systems deployed on the server or client, the network resources allowed to access, the strength of security needed, performance issues and administrative overhead. Before we install any security solution we need to choose the right one .The main criteria to compare different VPN solutions should be based on; availability, Network security, scalability, quality of service (QOS) and management**.** [17]

In this section I am going to compare and contrast and show the main advantages and disadvantages of some of the main VPN protocols like PPTP, IPSec, SSL, L2TP and SSTP.

3.1 Advantages and Disadvantages of PPTP

PPP has the following advantages and disadvantages.

Advantages:

- Provides encryption strength of 128-bit.
- Promotes nearly all VPN supported operating systems.
- It is friendly with all platforms.
- The setting is easy and simple.
- It is faster because there is no encryption.
- There is no terminal authentication.
- It is relatively cheap mainly because, it has an easy installation and does not cost much to use certificates.
- It does not require public key infrastructure.
- It uses routing and remote access. [17]

Disadvantages:

- There is no encryption in this protocol.
- The encryption in this protocol begins when the machines have gone through the authentication step and establish the point-to-point link.
- It needs to perform authentication on user level.

- Less security level.
- There is some lack of agreement with the Generic-Routing-Encapsulation (GRE).
- Dependent on the complexity of the password used to authenticate the PPTP connection.
- Provides a tunnel but no encryption.
- Does not provide data integrity and it does not verify the sources of data so, we cannot confirm whether the data is authentic or not. [17]

3.2 Advantages and Disadvantages of IPSec

IPsec has the following advantages and disadvantages.

Advantages:

- Provides encryption strength of 256-bit and uses tunnel and transport for the sake of encrypting.
- Relative to PPTP it produces much better encryption. It is believed that it is a well secured and authentic VPN protocol.
- The setup is easy and steady.
- Provides a higher level of security.
- Uses encryption as well as authentication of machine and user.
- Provides data confidentiality and integrity.
- Provides high security, requires public key infrastructures.
- Uses Routing and Remote access.
- Being easy to keep up and better security makes it standard at international level.
- It came up with out of sight technology and its process never has to be learned by its users.
- In this protocol there is no compatibility question, the main reason is all the implementations are network layer.
- Provides integrity.
- Terminal authentication with Md-5, IKE with pre-shared key or digital certificates.
- For a user authentication it uses Digital certificates and mutual authentication secret passwords.
- There is no need for installation of client software. [17]

Disadvantages:

- More difficult to install and utilize the security certificate.
- Greater processing speed is required. [17]

3.3 Advantages and Disadvantages of SSL

SSL has the following advantages and disadvantages.

Advantage:

- Provides confidentiality and integrity.
- Variable and strong encryption.
- Good security.
- Digital certificates HTTP authentication.
- Uses digital certificates for user authentications.
- On the client site installing soft ware is not needed.
- This protocol protects our online information and since we need no software one the client side it reduces the cost. [17]

Disadvantages:

- The performance of this protocol is slow since the encrypted files use most of the resources of the server.
- If a user sends his credit card to other user over SSL and if the receivers' server is not secured, the personal information of the sender might get hacked. Hackers might easily break and gate the sender's information and such a kind of data crack happens frequently. [17]

3.4 Advantages and Disadvantages of L2TP

LT2P has the following advantages and disadvantages.

Advantage:

- Since it provides the most decent encryption, it gives reliable security for sensitive information and applications.
- L2TP uses two layers of encapsulation.
- It gives cost effective, efficient and better connection.

- It is easy to use and the setting up is simple.
- This protocol can be used on all recent platforms.
- It is reliable, rapid, adjustable, scalable and genuine.
- For authentication sake it gives the finest approval policy for users.
- This protocol collaborates with IPSec to give 168-bit encryption.
- It needs two levels of authentication that makes it better than PPTP regarding encryption.
- The encryption of authentication process makes it impossible to listen in the transmission.
- If we prefer to have secured VPN than speed this protocol is preferred. [17]

Disadvantages:

- Since it encapsulates the data twice it makes the speed slow.
- It uses pre shared keys and miss match between the keys occur sometimes.
- This protocol provides a very good security with slow speed .The slow speed is because of the usage of CPU in the encryption process .[17]

3.5 Advantages and Disadvantages of SSTP

SSTP has the following advantages and disadvantages.

Advantage:

- It is meant for remote customer accesses.
- It uses SSL with the addition of data encryptions and data transmissions.
- It is considered as the most reliable protocol because it makes use of SSL plus authentication certificates and 2048-bit for encryptions.
- It makes sure that the data is always secured. [17]

Disadvantages:

- It is only compatible with window 7 or recent version.
- The data transmition speed is very slow relative to other VPN protocols. [17]

Table 4 summarizes the advantages of some of the selected VPN solutions. It covers the assessments based on speed, integrity, confidentially, encryption and stability.

Table 4.Comparison of different VPN solutions

	IPSec site-to site	IPSec server-client	SSLclientless	PPTP	L2TP	SSTP
Speed	Fast	Fast	Yes	Fast	Fast	Fair
Integrity	Yes	Yes	Yes	no	Yes	
confidentiality	Yes	Yes	Yes			
Encryption/security	Fair	Fair		low	Acceptable	Acceptable
Stability	Acceptable	Acceptable	Yes	Fair	Acceptable	Fair
COST	High	High	low	low	low	

4 Securing Network and Implementation of VPN Models

4.1 Methodology

For testing I used two methods. The first is Cisco configuration professional and the second is command line interface. I prepared a topology and configured the VPNs based on it.

CCP (Cisco configuration professional) is a tool that helps to secure a network. It uses protocols like Secure Shell and HTTP which makes it more secure. Cisco configuration professional is used only on Cisco products. The first thing to do before using CCP is creating a community and adding the routers. The community is a group of selected devices with a maximum capability of 10 devices. We are required to enter the IP address, host name and every credential of the router to add it to the community.

I chose to use both Cisco configuration professional and command line. Cisco configuration professional is easy to manipulate and we can use it for almost all VPNs. It also helps during configuration.

4.2 Network-Based VPN Testing

In this network-based testing, I used the topology in figure 10. I took an imaginary company which used to have only one main office and after a couple of years they planned to expand their primary market. The company decided to open a remote branch office a few kilometers away from their main office. The branch office will be considerably smaller than the main office in this network topology. As shown below in figure 10 I used packet tracer to make the topology .The main objective was to connect the workers from R3 safely to the main office. The R3 needs to get an access to the main office services. In order to implement this I used Site-to-site, IPSec and SSL VPN on the main office.

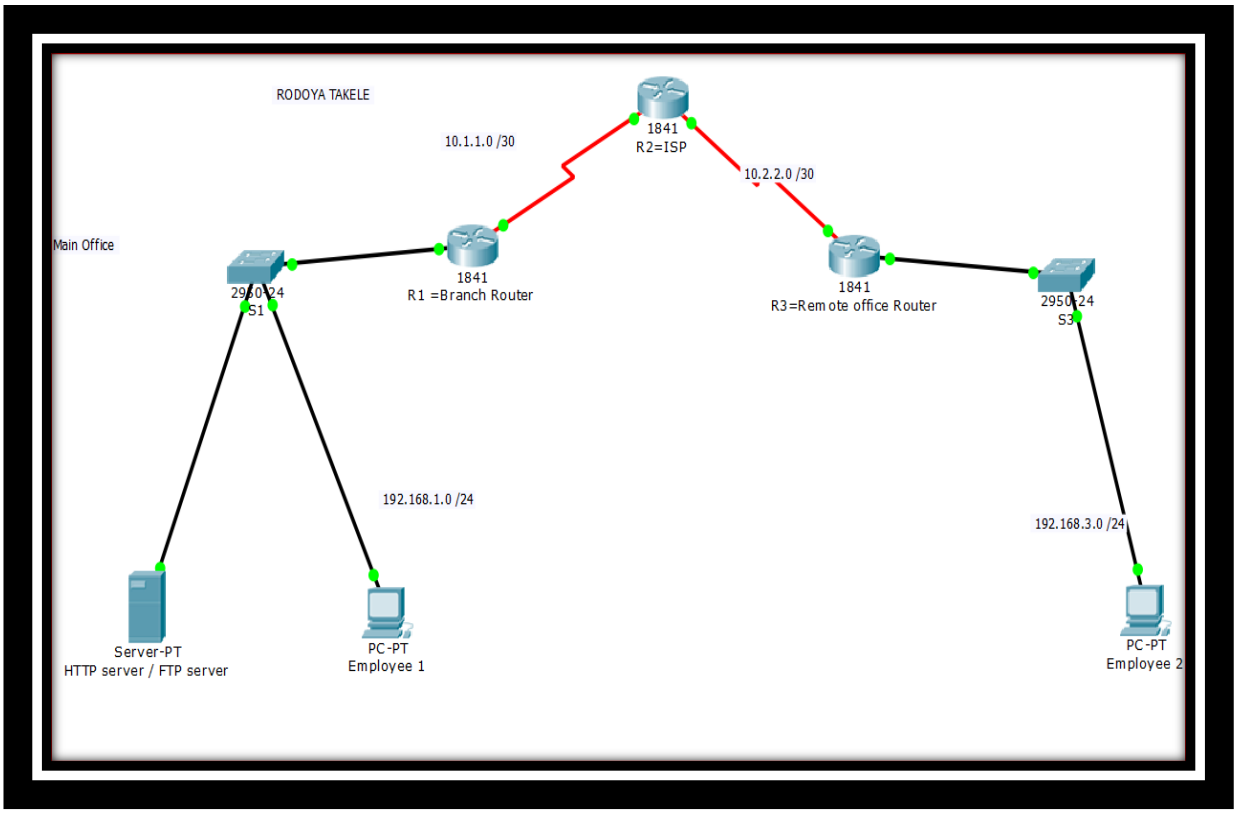


Figure 10.Simulated network topology of the company.

Basic Router Configuration

Based on the above topology I configured the basic router configuration, as shown in Appendix 1.

Enabling HTTP/HTTPS server

To enable the HTTP /HTTPS server I configured the routers which are in configuration mode as shown in listing 1;

```
Router (config) #ip http server
Router (config) #ip http secure-server
Router (config) # ip http authentication local
```

Listing 1.Enabling HTTP/HTTPS server

Creating a privileged user account

To create a privileged user account I used a user name and password as shown in listing 2;

```
Username admin privilege 15 password cisco12345
```

Listing 2.privileged user account

Configuring a SSH and Telnet access

To configure SSH and give telnet access I used vty line and telnet ssh as shown in listing 3;

```
Router (config) #line vty 0 4
Router (config) #login local
Router (config) #transport input telnet
Router (config) #transport input telnet ssh
Router (config) # exit
```

Listing3. Configuring a SSH and Telnet access

From R3 I stared the CCP on Employee 2 and entered our Remote branch office credentials. The next step was discovering the server and connecting R3. Figure 11 shows the remote office branch and illustrates now that the router is in the community and it is discovered.

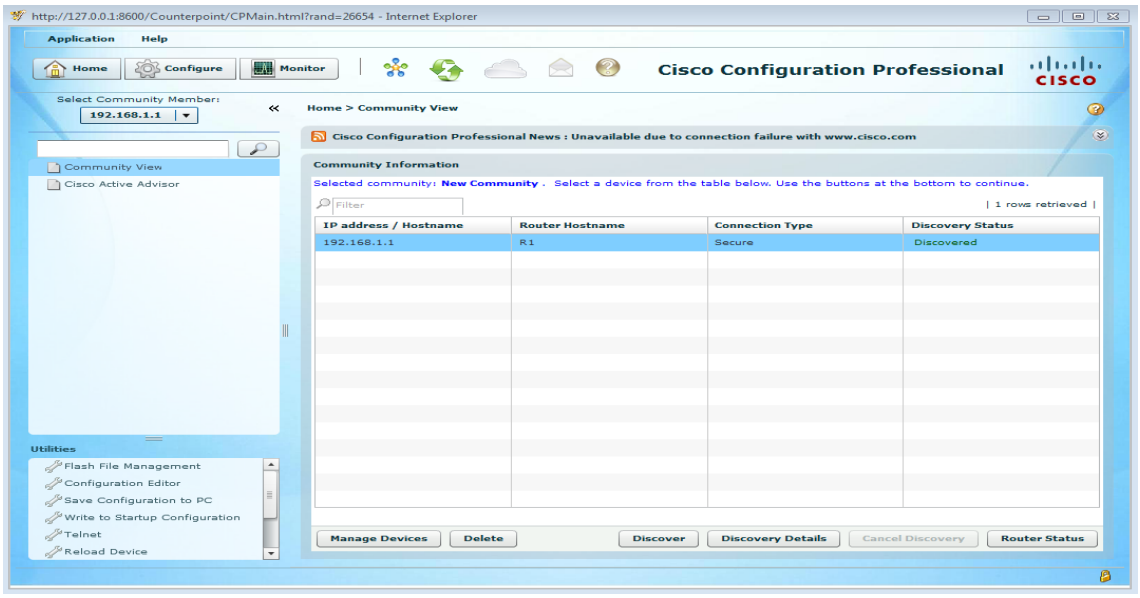


Figure 11.Remote office branch discovered.

And as expected the router is in the community and it is discovered.

4.3 Implementation of VPN Models

4.3.1 Application of Site-to-Site VPN

The site-to-site is also known as router-to-router VPN connection which is used to set a network connection in different offices of a company by using a common medium to securely transfer data. It is the exchange of packets between two routers in a different network through VPN connections. It is used to connect parts of two private networks. The first task was building a site-to-site VPN tunnel between the main office and a remote access router which passes through R2. To set up the IPSec VPN I needed to configure R1 and R3 using Cisco IOS and CCP. [9]

To set IPSec between these two routers, there are two main areas to configure;

- Configuring the Internet Key Exchange (IKE)
- Configuring IPSec parameters

An IPSec VPN negotiation steps below shows how a negotiation takes place to exchange information;

1. Employee 1 sends interesting traffic to employee 2
2. Then R1 and R3 will negotiate in an IKE phase 1
3. R1 and R3 will negotiate in an IKE phase 2

4. Data is exchanged through IPSec tunnel
5. Finally IPSec is terminated [16]

The main steps used to configure a site-to-site VPN and the pictures are shown and explained below.

The first step is in order to start configuration is opening the VPN wizard and selecting the step-by-step wizard. The step-by-step wizard is quick to set up and provides default configuration. Figure 12 shows that I choose the step-by-step to continue the configuration.

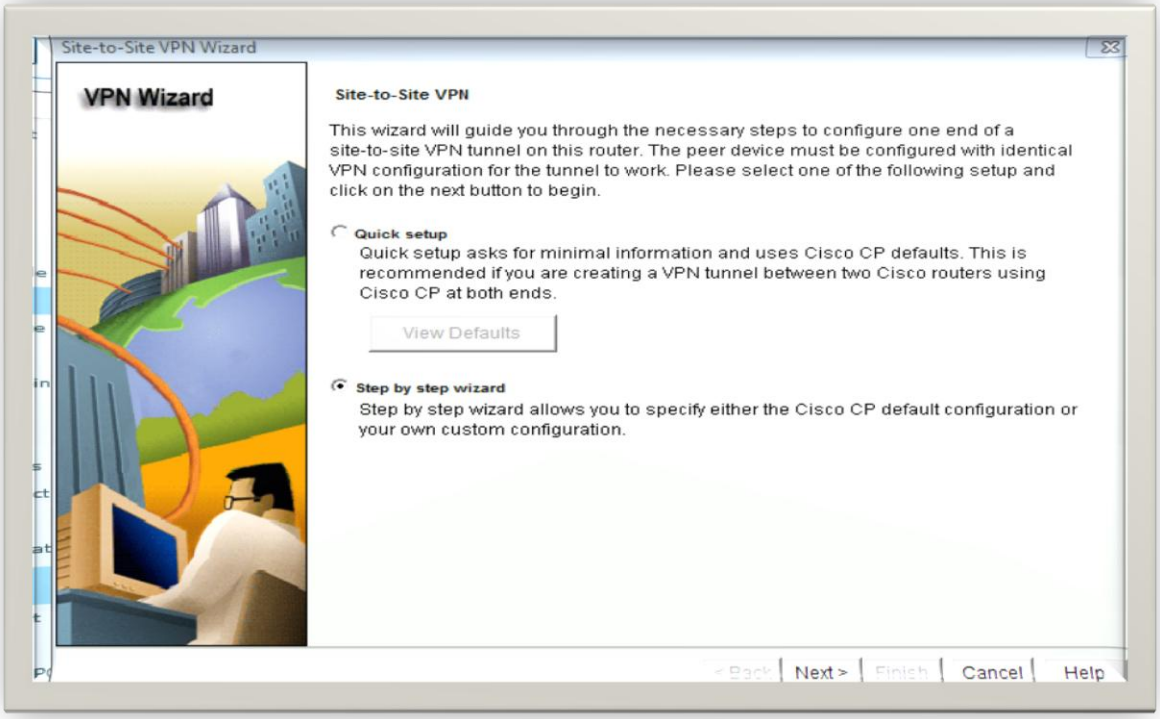


Figure 12.The first step in site-to-site configuration.

In the second step as shown in figure 13 I was required to enter the credentials in the required spaces. It is also required to select the right interface for the VPN connection. Here, serial 0/0/0 was selected. In the next section I selected the peer with static IP address and provided the remote office IP. Then in the authentication section it is required to enter the pre shared keys.

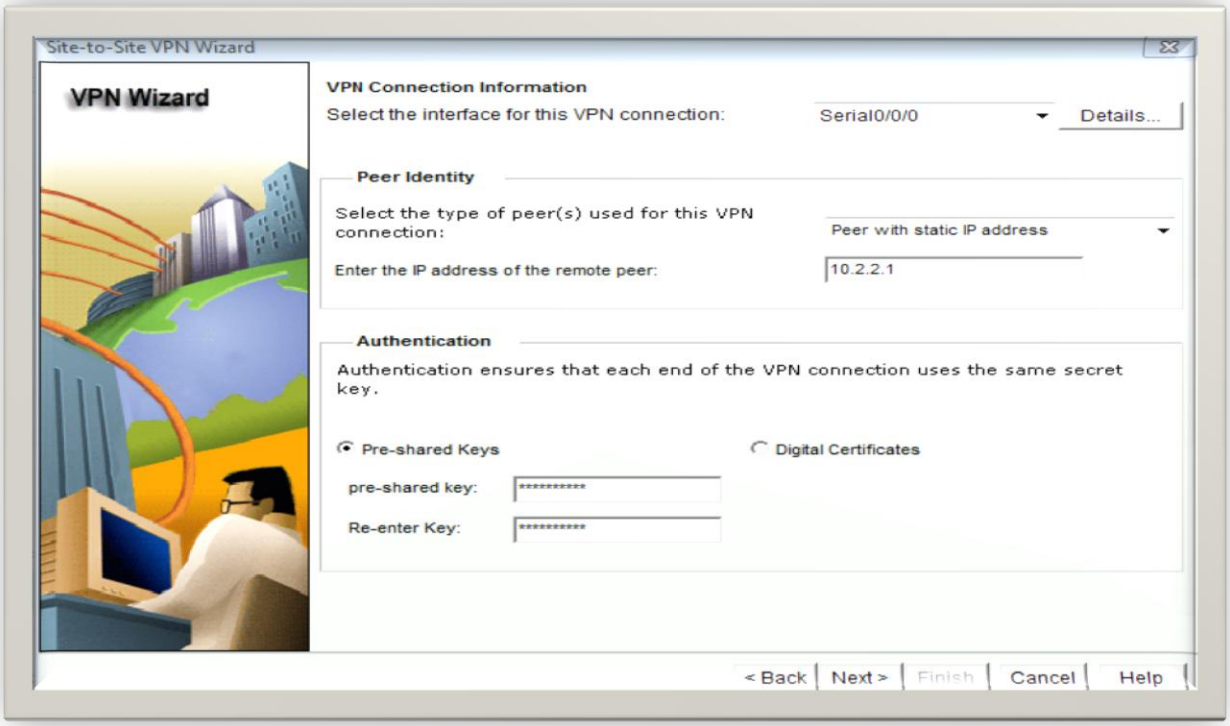


Figure 13.VPN connection information.

As shown in figure 14 in the IKE proposal page I added the proposal that defined the algorithms and the methods for key exchange. The algorithms are encryption, authentication and key exchange methods. The values need to be the same with the values in the remote office router (R3).

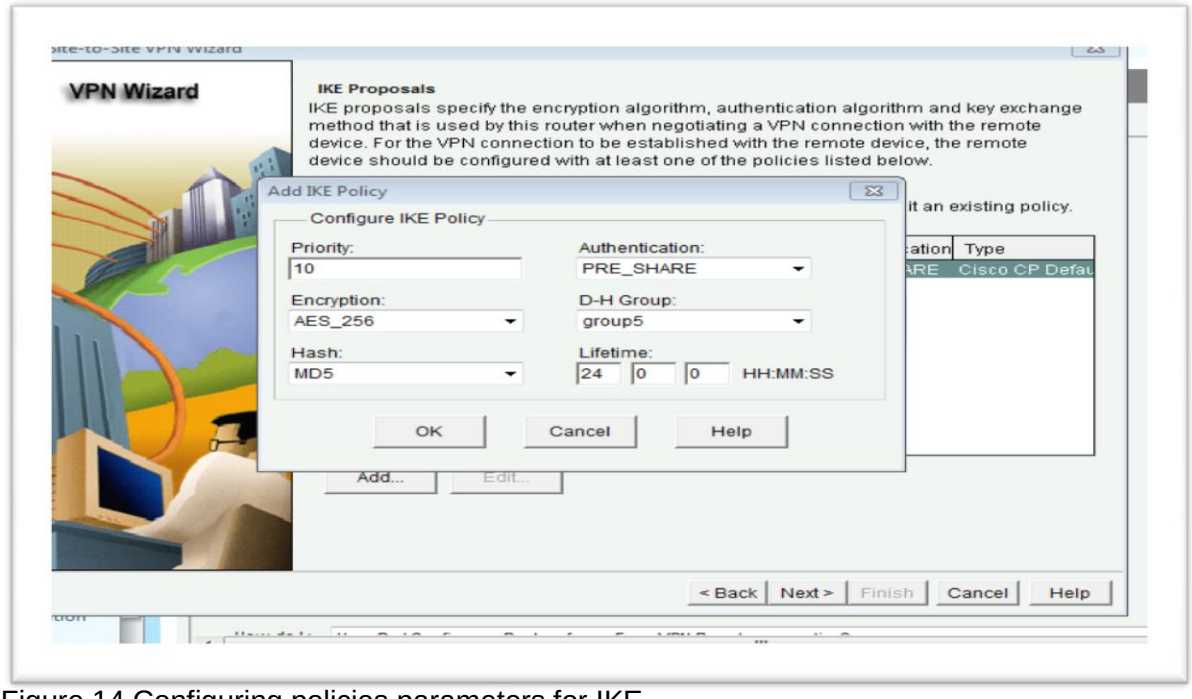


Figure 14.Configuring policies parameters for IKE

The Transform set is an IPSec policy which we can use for encryption, hash, and authentication data. In this section and in figure 15 the details about the transform set are given. They are integrity and encryption algorithms. Here the algorithms can be manipulated to secure the information passing through the VPN tunnel. We can add any information and the number of required transform set.

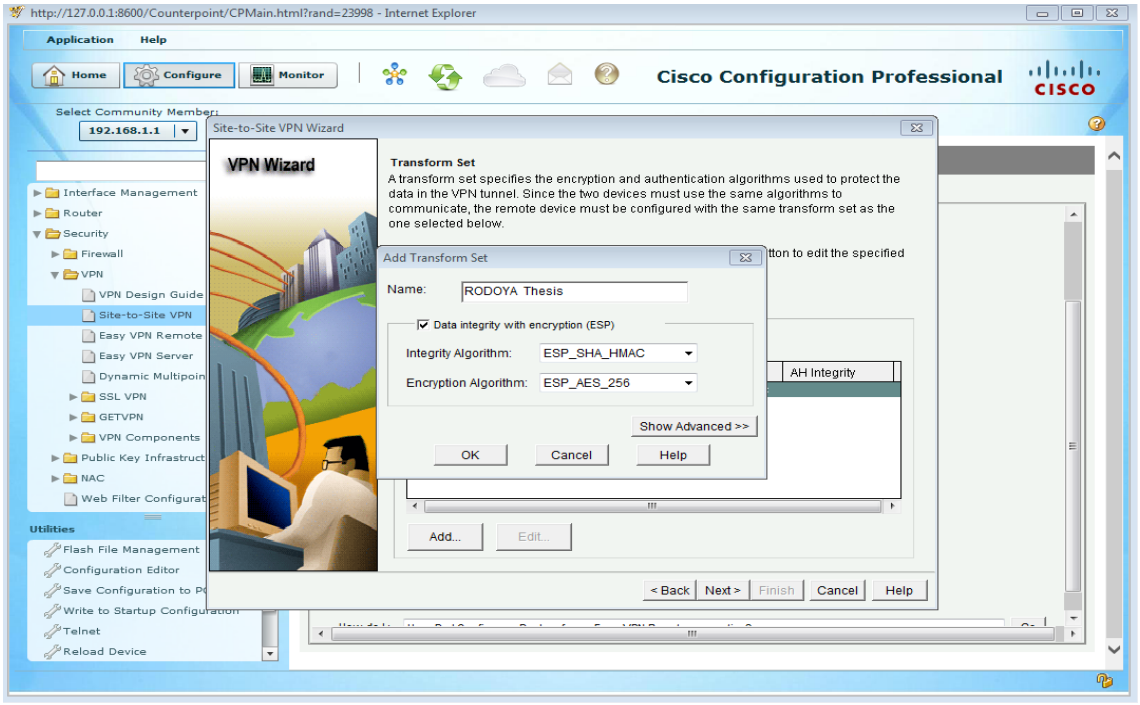


Figure 15.Configuring transform set

The next step is summarizing what I did as shown in figure 16. We do not need to check VPN connectivity before we create a mirror image on our R3 to finish and move to the next page.

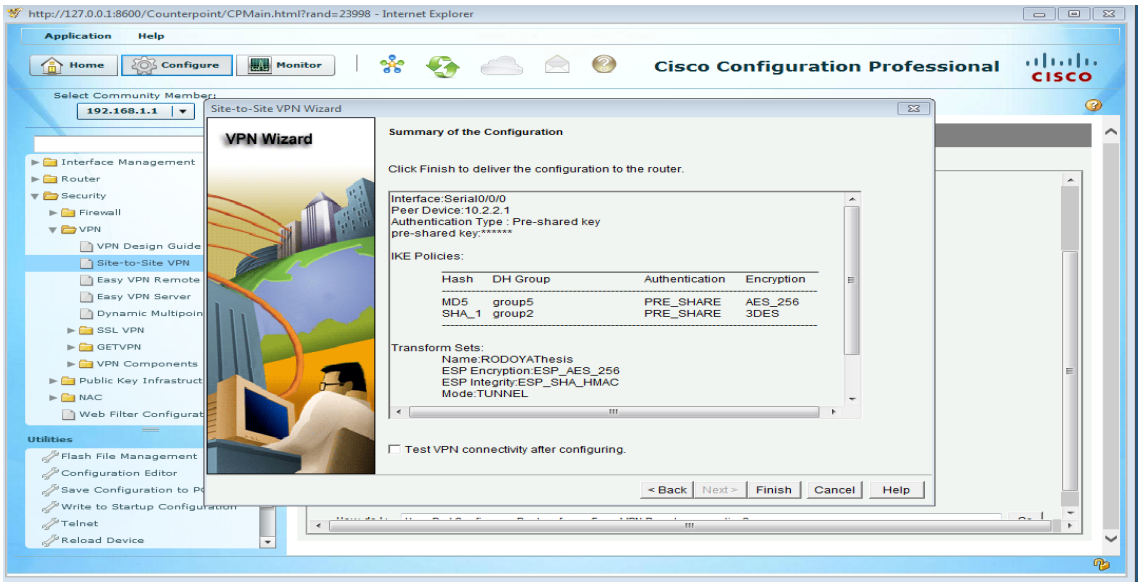


Figure 16.Checking summary of the configuration

After reviewing the configuration the next window is delivering the configuration. In figure 17 I checked in the save running button and pressed the deliver button to complete the work.

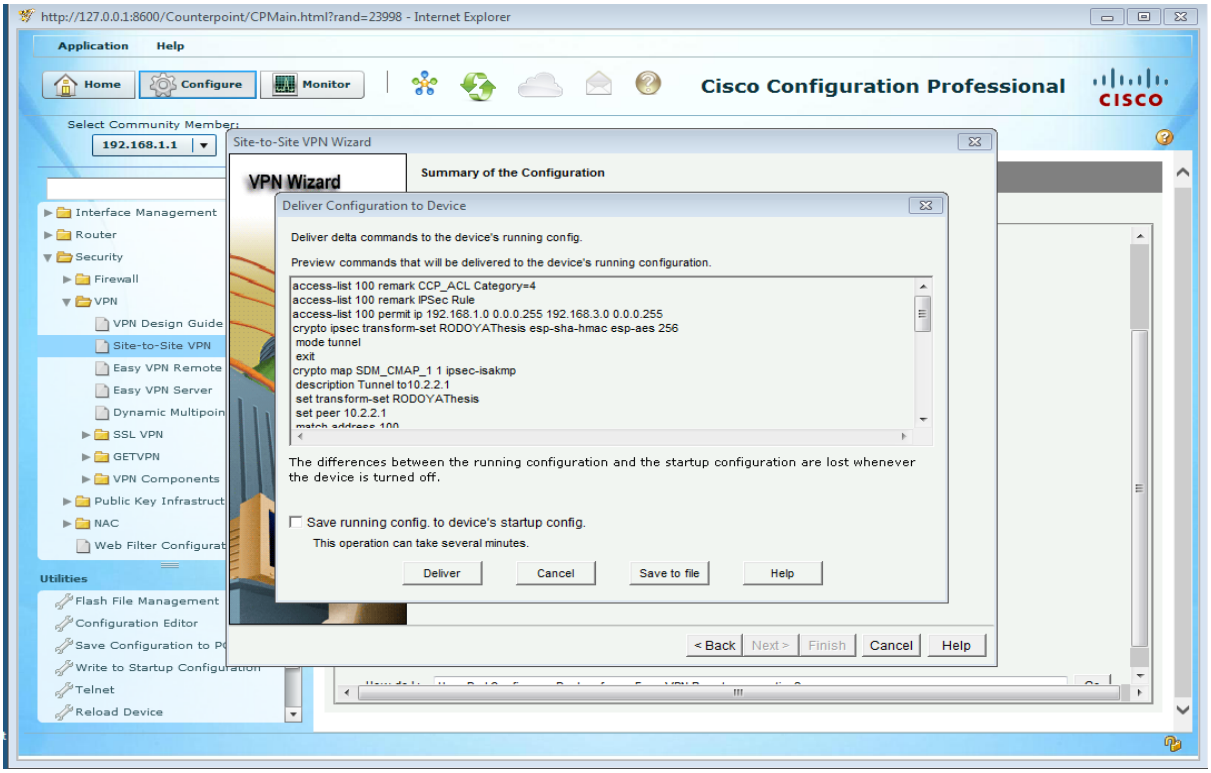


Figure 17.Delivery of the summary

After I completed the delivering the screen comes with command delivery status. Figure 18 shows the summary and delivery status.

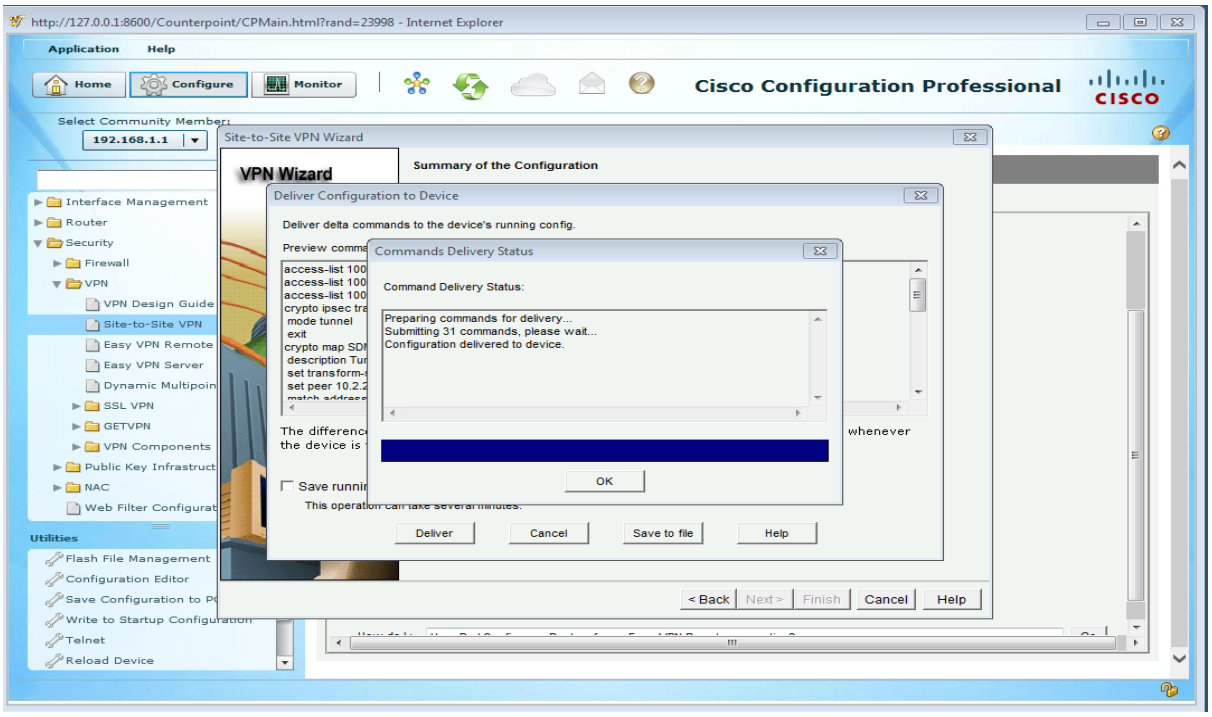


Figure 18.The status of delivery.

As shown below in figure 19 the tunnel was still dawn. To make the tunnel up I was required to create a mirror configuration on R3.

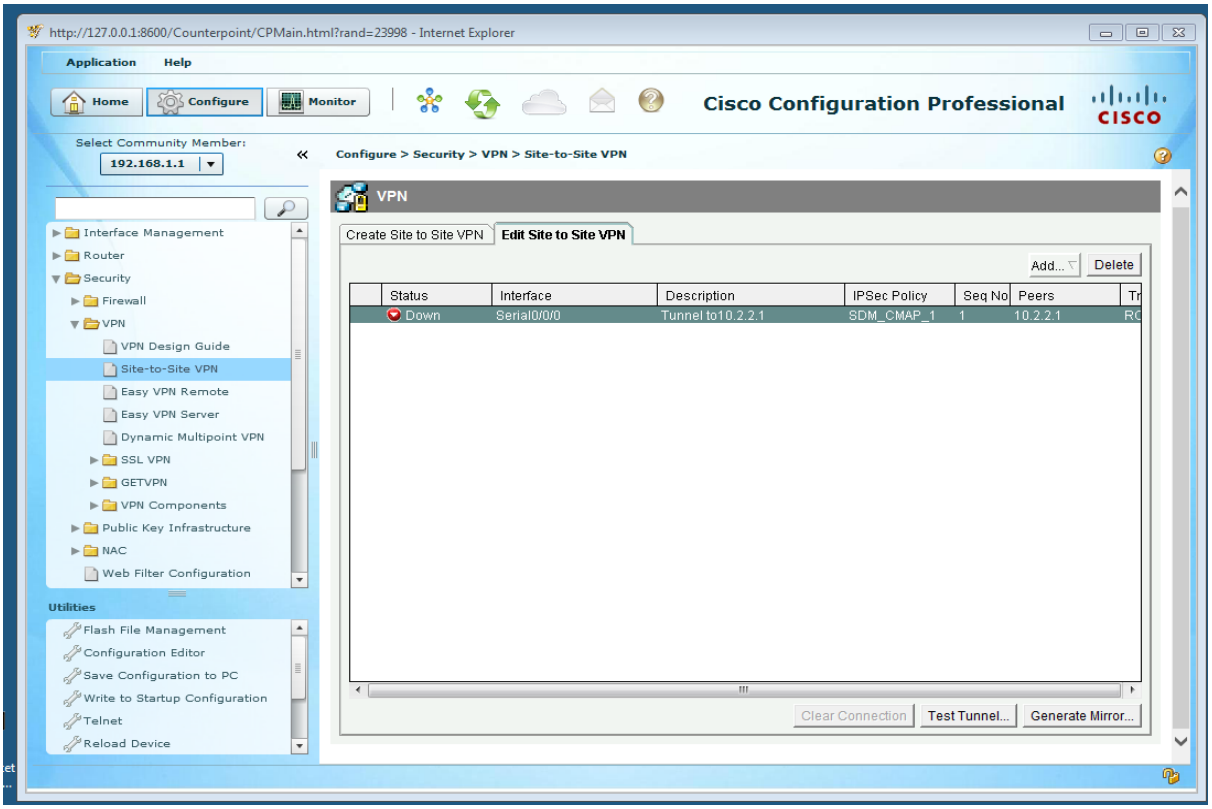


Figure 19.The tunnel still not fully configured.

As mentioned above in order for the tunnel to become up it is needed to generate a mirror configuration on R3.The generated mirror configurations are listed in appendix 2 and the image is shown below on figure 20.I saved this configuration and apply it on R3.

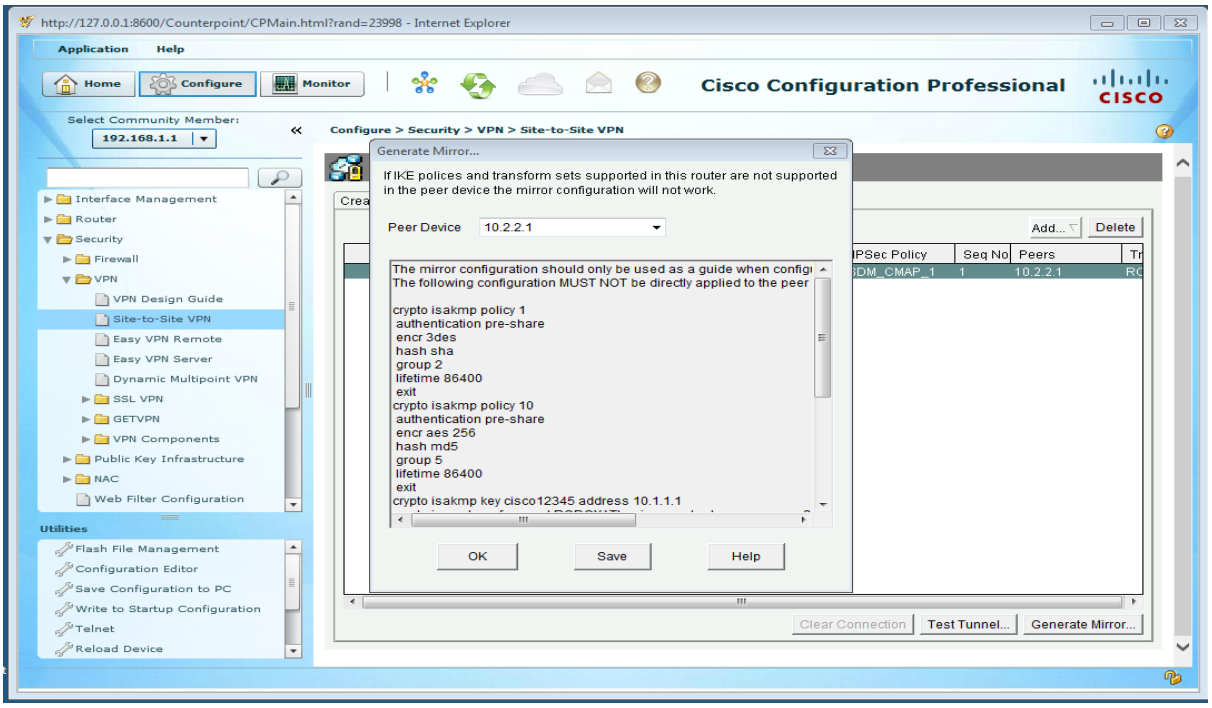


Figure 20 .Generating mirrors on R1

To test the connectivity of the VPN I started troubleshooting. As shown in figure 21, the router starts debugging which generates traffic in the tunnel. Then it requests to enter the destination IP which is 192.168.3.1 to begin the debug.

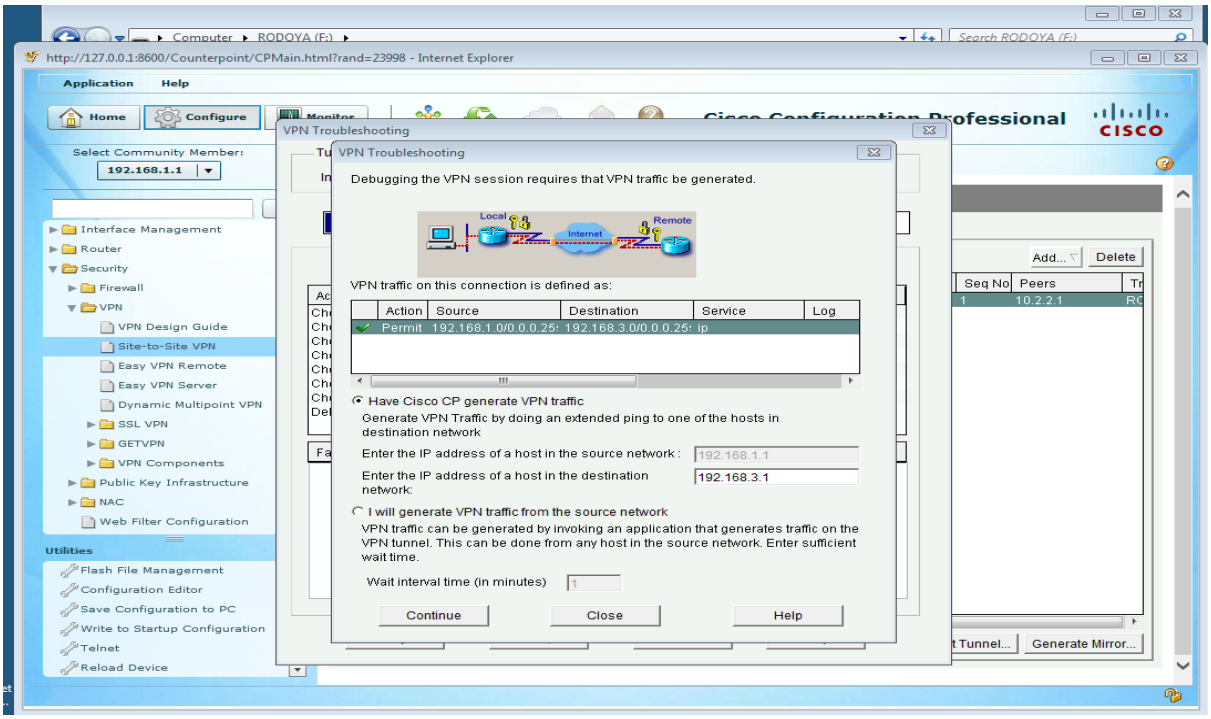


Figure 21.Trouble shooting of VPN

The above debugging continues and it was a success that means the required tunnel is up. As shown in figure 22 the tunnel was successful and up.

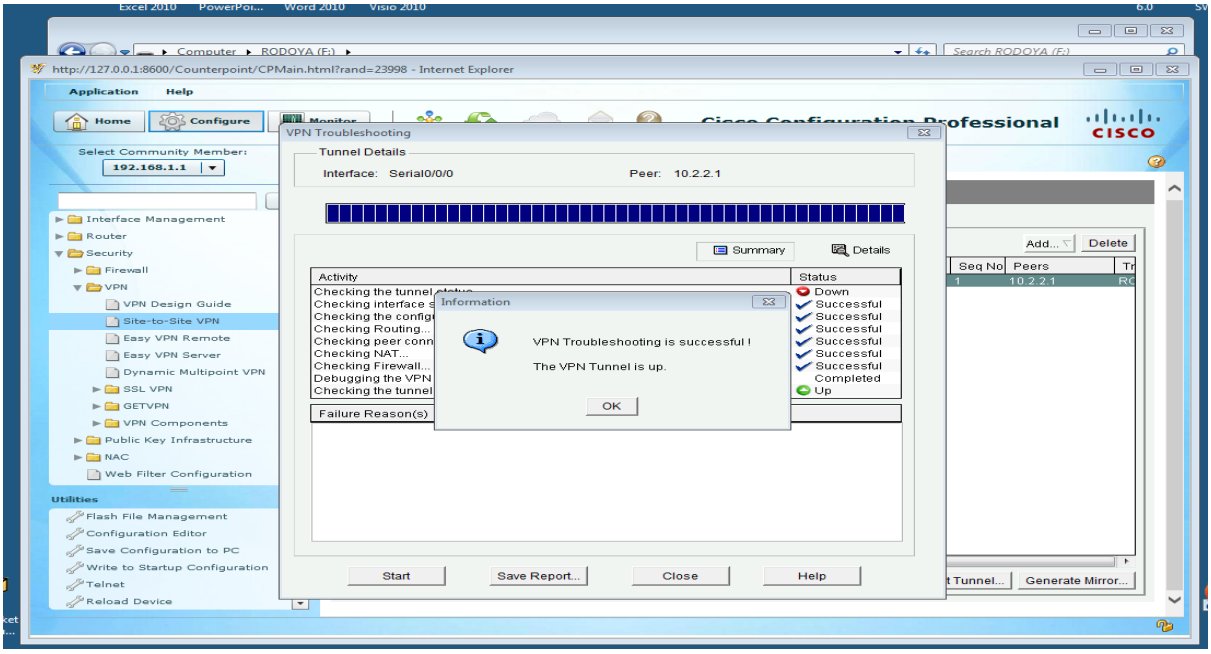


Figure 22.VPN site to site tunnel is successfully enabled

The following commands were configured on the main office router or R1 and remote office R3; [3]

Crypto isakmp enable

For IPSec to function we need to enable IKE. Listing 4 makes IKE enable. Though it is enabled automatically, sometimes it might be disabled for some reason.

```
R1 (config) #crypto isakmp enable
R3 (config) #crypto isakmp enable
```

Listing 4.Enabling Crypto isakmp

The IKE Phase 1 negotiations which define the key exchange used to validate IKE policies between R1 and R3. Listing 5 shows the IKE phase 1 negotiations. [3]

```
R1 (config) #crypto isakmp policy 10
R1 (config-isakmp) #authentication pre-share
R1 (config-isakmp) #encryption aes 256
R1 (config-isakmp) #hash sha
R1 (config-isakmp) #group 5
R1 (config-isakmp) #lifetime 3600
R1 (config-isakmp) #end

R3 (config) #crypto isakmp policy 10
R3 (config-isakmp) #authentication pre-share
R3 (config-isakmp) #encryption aes 256
R3 (config-isakmp) #hash sha
R3 (config-isakmp) #group 5
R3 (config-isakmp) #lifetime 3600
R3 (config-isakmp) #end
```

Listing 5. IKE Phase 1 negotiations

Configuration of pre-shared keys is the next step shown in listing 6 and they are very important as they are used to authenticate in the IKE policy; [3]

```
R1 (config) #crypto isakmp key cisco123 address 10.2.2.1
R3 (config) #crypto isakmp key cisco123 address 10.1.1.1
```

Listing 6. Pre-shared key configuration

The other basic configuration shown in listing 7 is IPsec transform set which is used by the routers to negotiate and form a secured tunnel. It also specifies the cryptographic algorithms and functions which help routers. [3]

```
R1 (config) #crypto IPsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#mode tunnel
R1(cfg-crypto-trans)#exit
R1 (config) #crypto IPsec security-association lifetime seconds 1800

R3(config)#crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)#mode tunnel
R3(cfg-crypto-trans)#exit
R3 (config) #crypto IPsec security-association lifetime seconds 1800
```

Listing 7. Transform set configuration

The next important step shows listing 8 which is encryption of traffic going from main office to R3.I extended the access list to be encrypted so that they are not going to be dropped if they are included in the access list. If there is no access list IP sec will not be able to form interaction with the two routers. [3]

```
R1 (config) #access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R3 (config) #access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Listing 8. Access list

A crypto map is used to match an access list to the areas and most IKE and IPSec settings and listing 9 shows the configuration for crypto map.

```
R1 (config) #crypto map CMAP 10 IPsec-isakmpf
R1 (config-crypto-map) #match address 101
R1 (config-crypto-map) #set peer 10.2.2.1
R1 (config-crypto-map) #set pfs group5
R1 (config-crypto-map) #set transform-set 50
R1 (config-crypto-map) #set security-association lifetime seconds 900
R1 (config-crypto-map) #exit
```

```
R1 (config) #interface S0/0/0
R1 (config-if) #crypto map CMAP
R1 (config) #end

R3 (config) #crypto map CMAP 10 IPsec-isakmp
R3 (config-crypto-map) #match address 101
R3 (config-crypto-map) #set peer 10.1.1.1
R3 (config-crypto-map) #set pfs group5
R3 (config-crypto-map) #set transform-set 50
R3 (config-crypto-map) #set security-association lifetime se-
conds 900
R3 (config-crypto-map) #exit
R3 (config) #interface S0/0/1
R3 (config-if) #crypto map CMAP
R3 (config) #end
```

Listing 9.Crypto map

4.3.2 Application of Remote Access IPSec VPN

Ipsec VPN secures a network by encrypting data. It can be either between a mobile user and a company or a remote user to a company through an internet provider. [9] I used SDM for this remote access IPSec VPN and the main steps were to configure a zoned-based firewall and the VPN client on a host. Configuring the VPN client on the host helps to set an end-to-end connection plus encrypted (IPSEC) VPN tunnels for users. Router R3 is the remote site, and R1 is the main office. Employee 2 represents an employee who wants to access the resources of the company; it could be from home or another location. Router R2 has no knowledge of the VPN connection passing through it and it also represents an Internet ISP router. R1 (main office) is configured as a VPN server and Employee 2 is configured as a Cisco VPN Client. [16]

The main steps used to configure Remote Access IPSec VPN are shown below and in figure 23. The detail of each step of the configuration is shown in Appendix 6;

- `R1 (config) #ip http server`, configuring ip http server on configuration mode enables HTTP server on the main office.

- `R1(config)#username admin01 privilege 15 password 0 admin01pass` ,user name and password is required to enables AAA (Authorization, Accounting and Authentication)

The configuration in figure 23 below shows enabling of http server on the main office router R1.

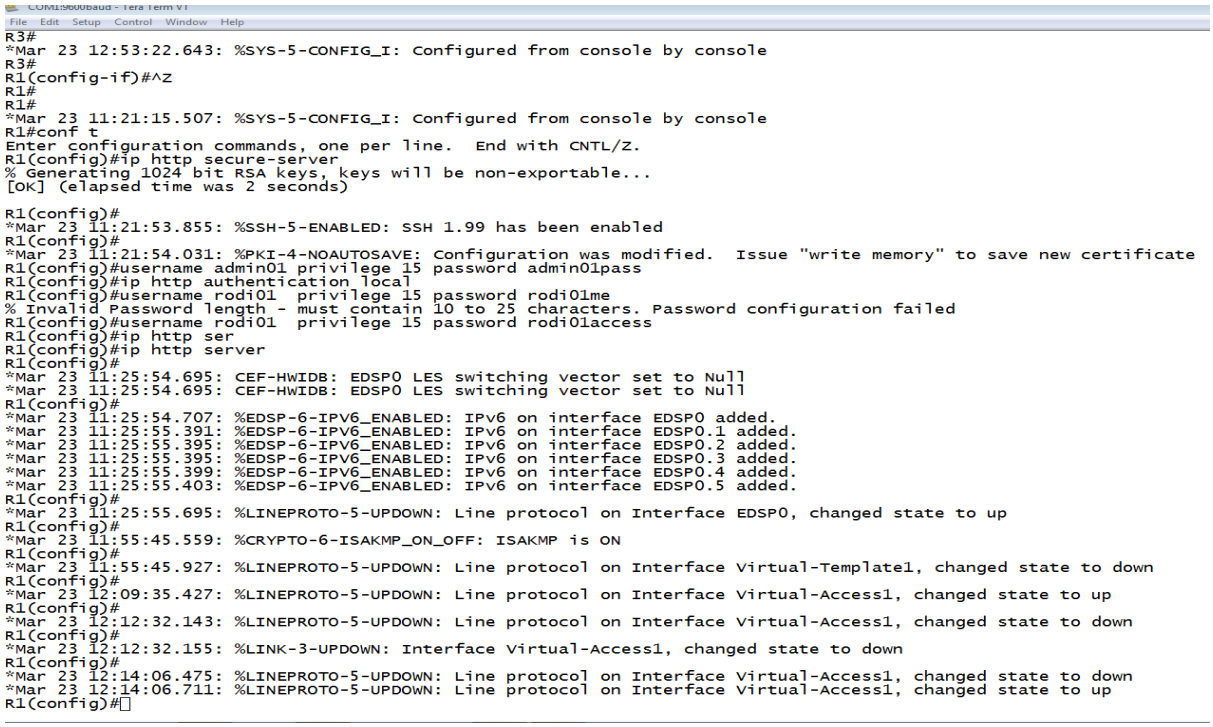


Fig 23.Enabling http on R1

Hyper text transfer protocol (HTTP) is used to enable the HTTP server on the system. Some of the basic steps are listed below:

- Easy VPN Server: used to set IPSec Client VPN and we configure AAA services first. Then defining local interface and authentication. Setting IKE proposals and Configuring transform set is very important part of the configuration since it specifies the policies and algorithms used in the tunnel.
- I selected a server for group policy lookup and enabled user authentication because whoever wants to access the server needs to authenticate and added user accounts.
- It is required to add at least one pool which will have the authorization and user group policies.

4.3.3 Application of SSL VPN

This VPN is used with a standard web browser. It needs to have a client software on users computer.SSL VPN is very important for tasks like file sharing, remote backup and remote system management. I was required to configure SSL on router R1 only .The major steps used are illustrated and every step of Cisco configuration professional is shown on Appendix 8. After selecting the SSL VPN manager, shown in figure 24 the first step was configuring the IP address and choosing the digital certificate. The IP address required helps to access the VPN and the certificates will help the authentication process.

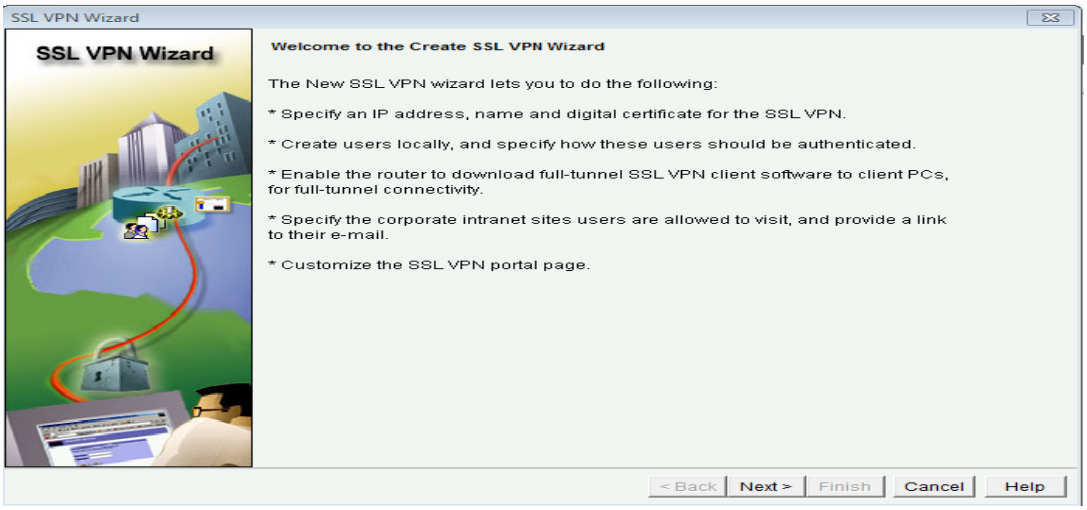


Figure 24.Summary of services provided by SSL VPN Wizard

I configured local or external user authentication as shown in figure 25 below. On the this step I was required to enter SSL VPN portal IP address, name and specified type of digital certificate used for authentication.

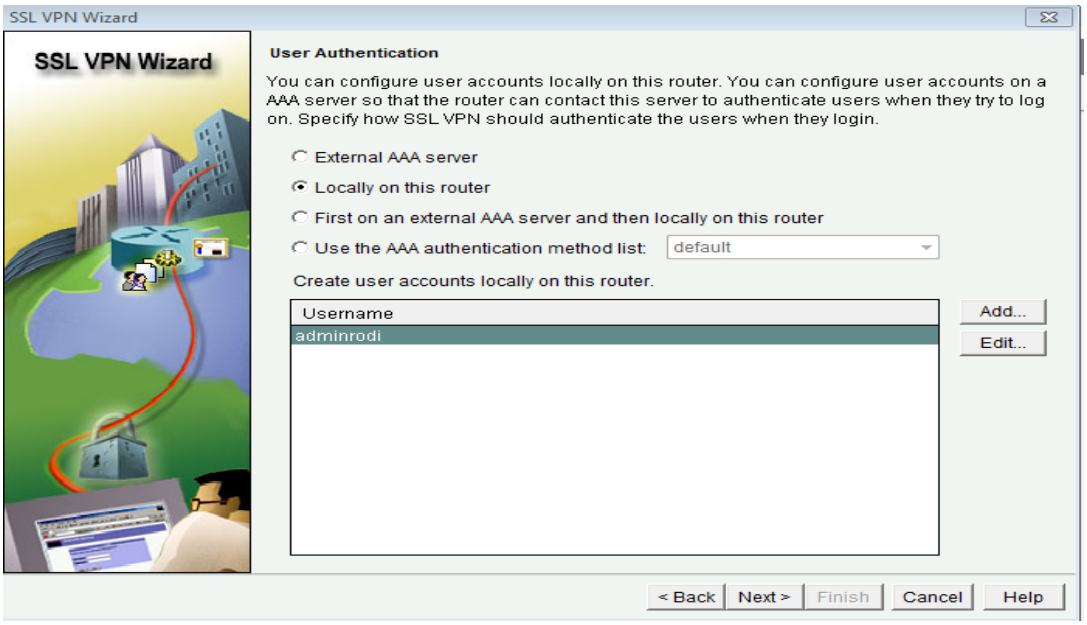


Figure 25. Configuring local or external user authentication

The very important step in this configuration is checking the summarization. It covers all the work we have done so far and figure 26 shows that the tunnel is up.

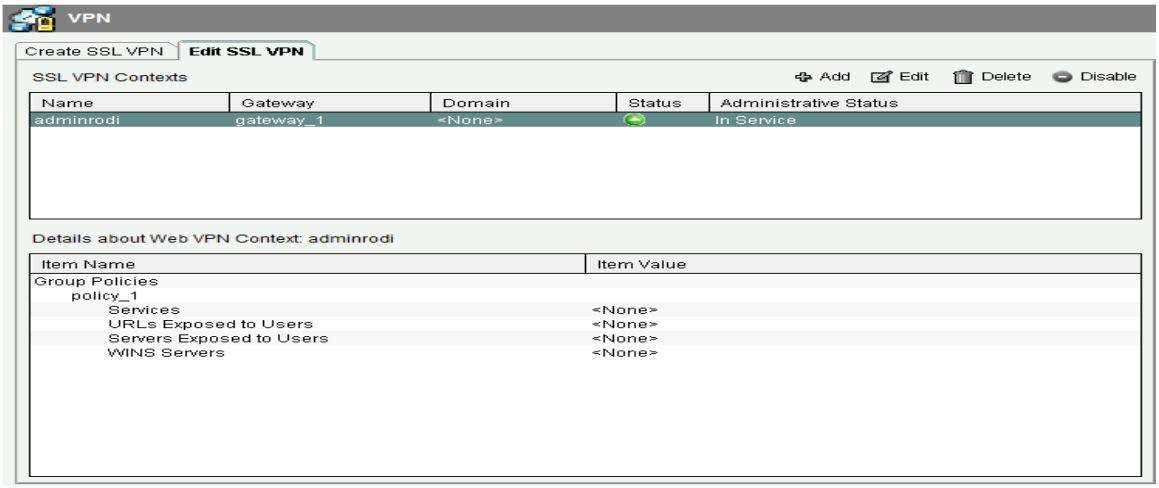


Figure 26.Successful VPN

The result was very satisfactory and this is the important step in this configuration. It summarized all the work we have done so far and now the tunnel is up.

4.4 Testing

In the testing section the above result is going to be assessed. The results obtained during the configurations above are also included here.

4.4.1 Testing Result of Site-to-Site VPN

The result below in figure 27 shows the application of crypto map to the R3 S0/0/1 interface and the output of the command show crypto isakmp policy. The show crypto isakmp policy command displays the policies configured on the router. It is needed to give crypto map set to the interface serial 0/0/1 since the traffic passes through it. The assigning of crypto map set to the serial 0/0/1 helps to manage all the traffic and identify the traffic against the crypto map set.

“Assigning a crypto map to an interface also initializes run-time data structures, such as the SA database and the security policy database. Reassigning a modified crypto map to the interface resynchronizes the run-time data structures with the crypto map configuration. Also, adding new peers through the use of new sequence numbers and reassigning the crypto map does not tear down existing connections.”[18]

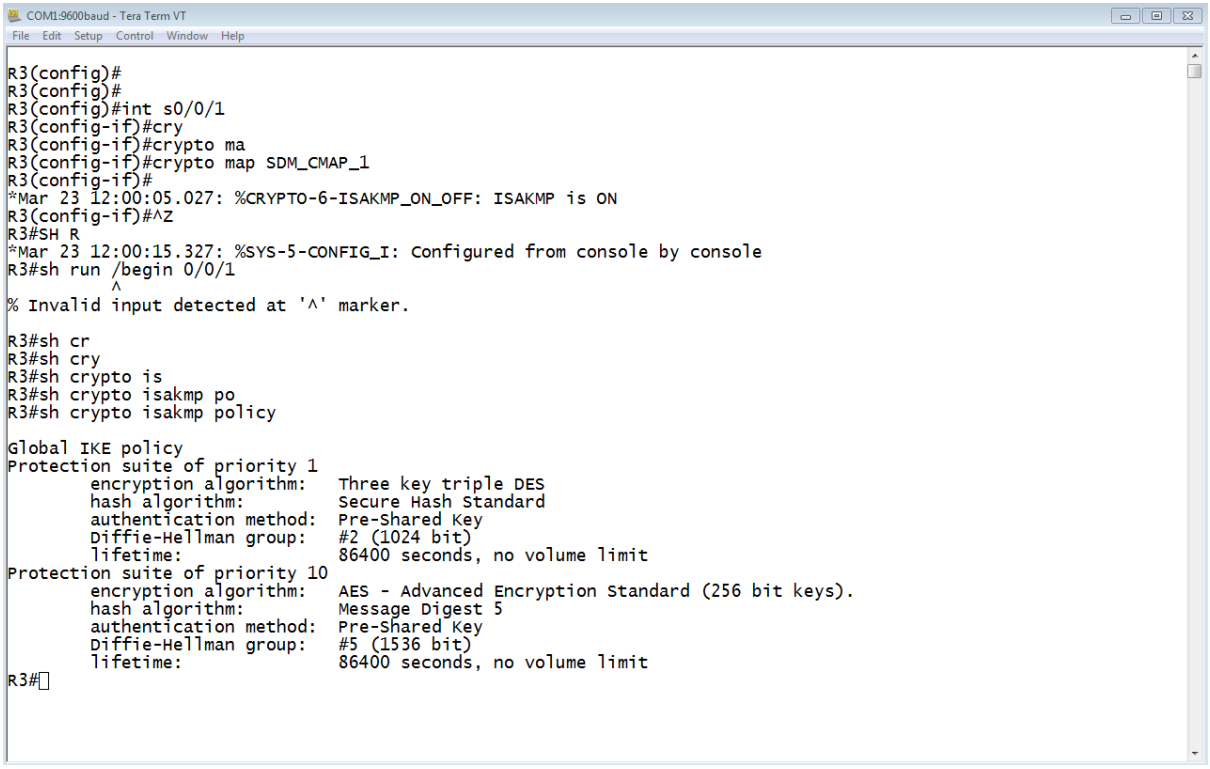


Figure 27.Crypto map and showing crypto isakmp policy

The output below in figure 28 verifies the configuration made on both routers and the commands I used to display the results are; show crypto isakmp policy, show crypto ipsec transform-set and show crypto map. Show crypto ipsec transform-set shows the configured transform sets. Figure 28 below it displays the algorithms used on the data passing through the tunnel. Show crypto map shows the crypto map configurations.

The show crypto isakmp policy shows two polices as shown. Figure 28 shows the result in which the first one is the one I configured and the other is a default configuration.

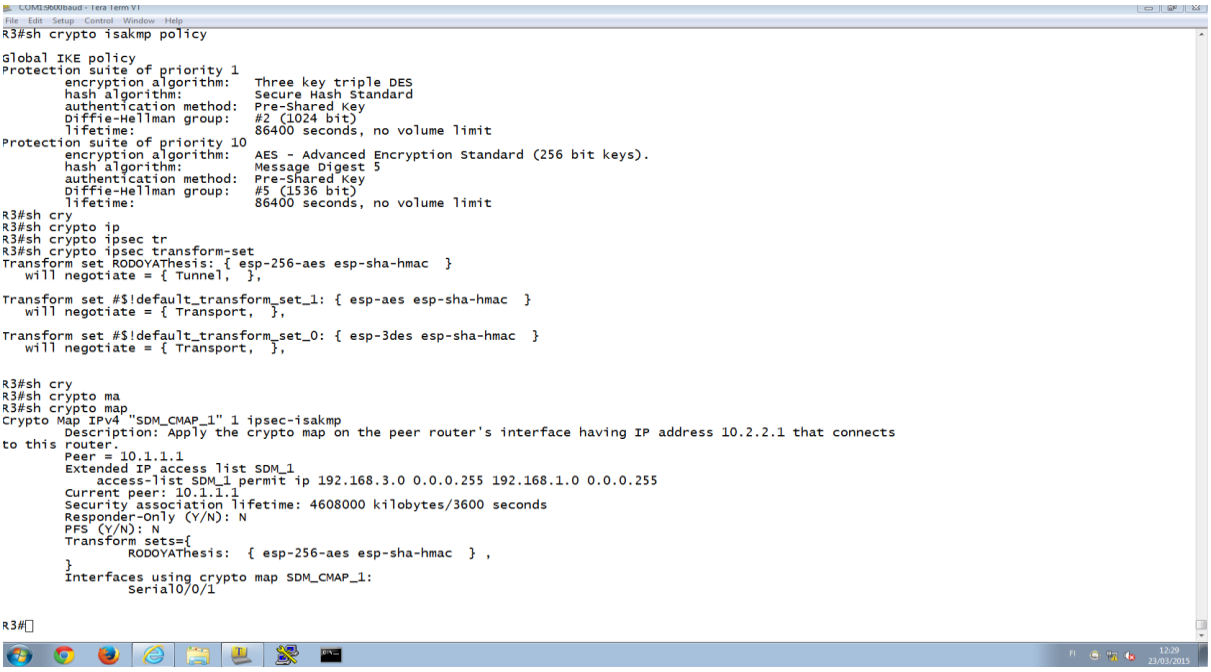


Figure 28.Result from the commands Crypto map and show crypto isakmp policy and transform set.

The result displayed above is from the commands show crypto map, show isakmp policy and show crypto ipsec transform set.

The SA is set up and as we can see in the figure 29 below packets are passing through the tunnel encrypted. The tunnel originates from the source 10.1.1.1 and ends at 10.2.2.1

```
R3#sh run int s0/0/1
Building configuration...

Current configuration : 89 bytes
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 crypto map SDM_CMAP_1
end

R3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.2.2.1        10.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

R3#
```

Figure 29.The result from the command Show run int s0/0/1

I continued pinging from R1 and run the command sh crypto ipsec SA as shown in figure 30 and the result was 29 packets transformed between the two routers.

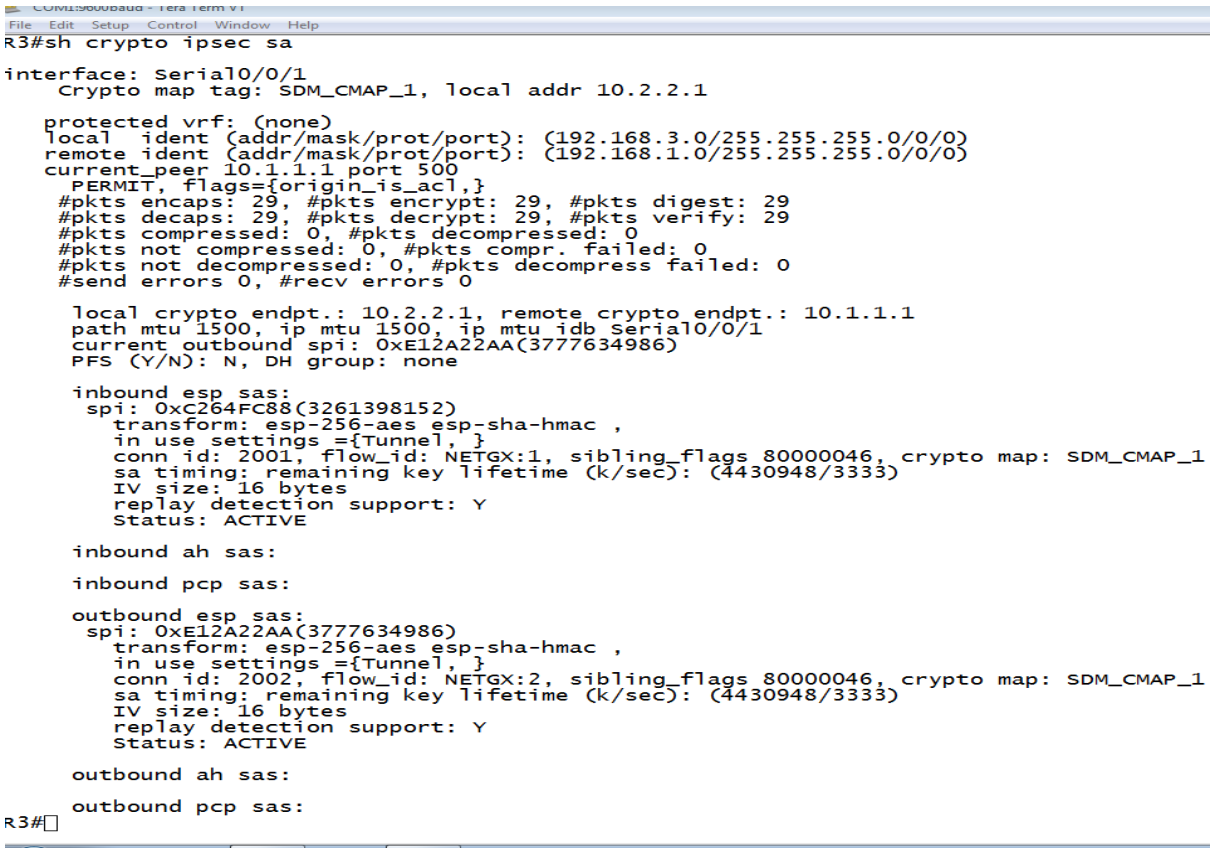


Figure 30.The result from the command show crypto isakmp SA

The following result in figure 31 shows testing of VPN using CCP. If the debugging is successful it means the tunnel is up. The screen shot below shows the result. The output shows the debug was successful and the tunnel is up.

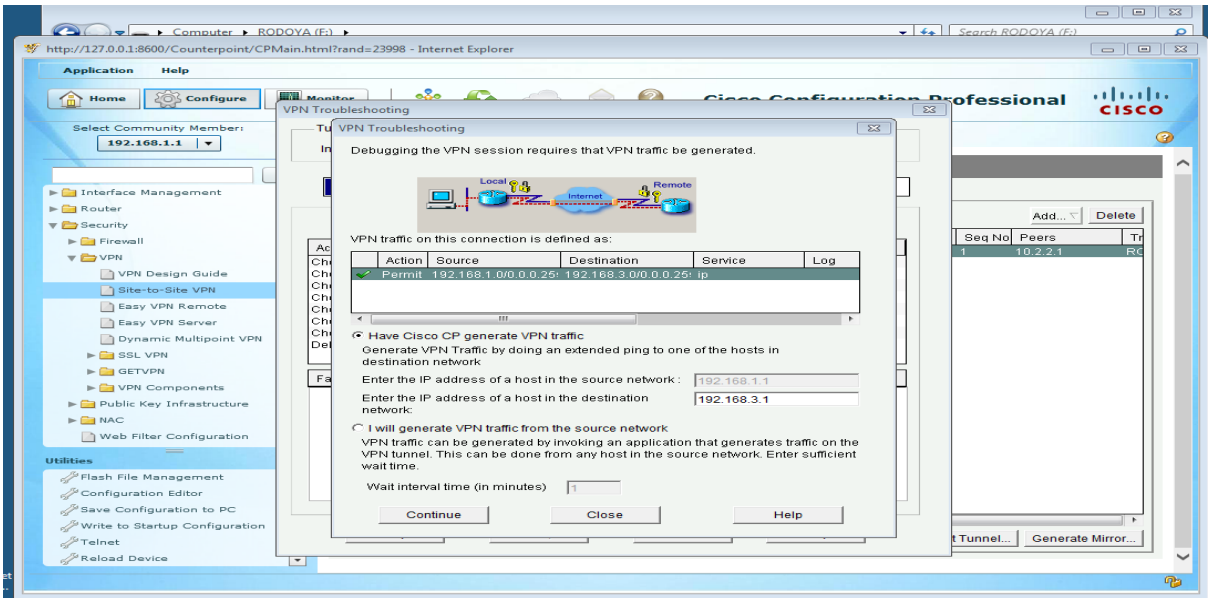


Figure 31.Testing using CCP

The output in figure 32 demonstrates the debug was successful as shown below and proves that the tunnel was up.

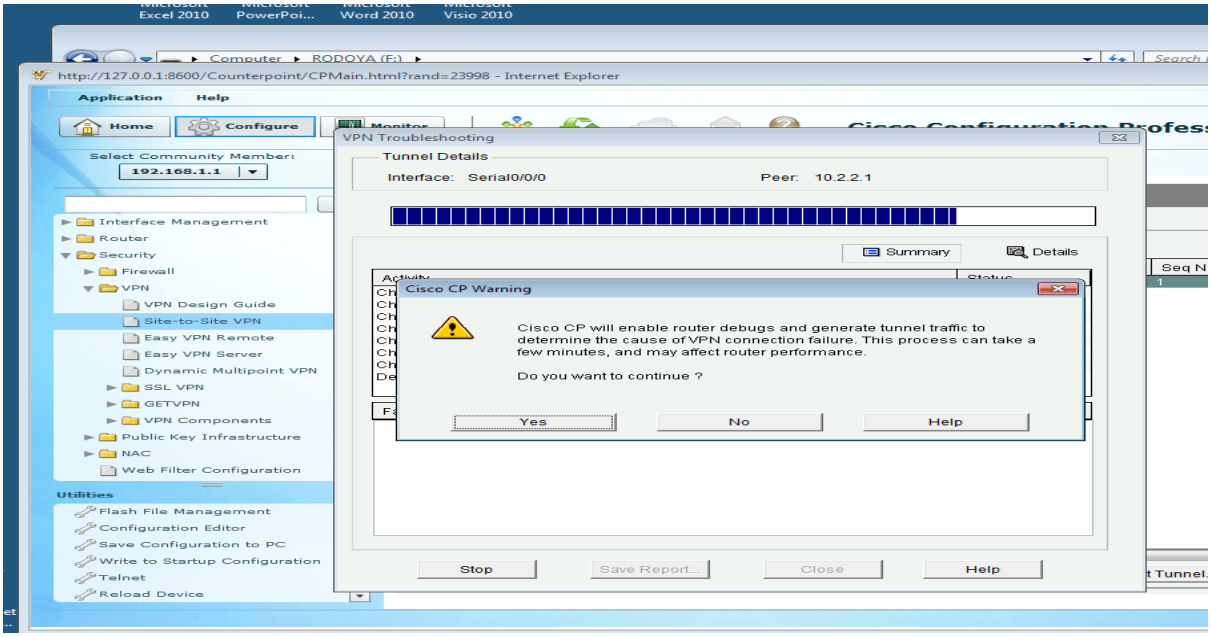


Figure 32.The debugging

Finally figure 33 shows now the VPN tunnel is up.

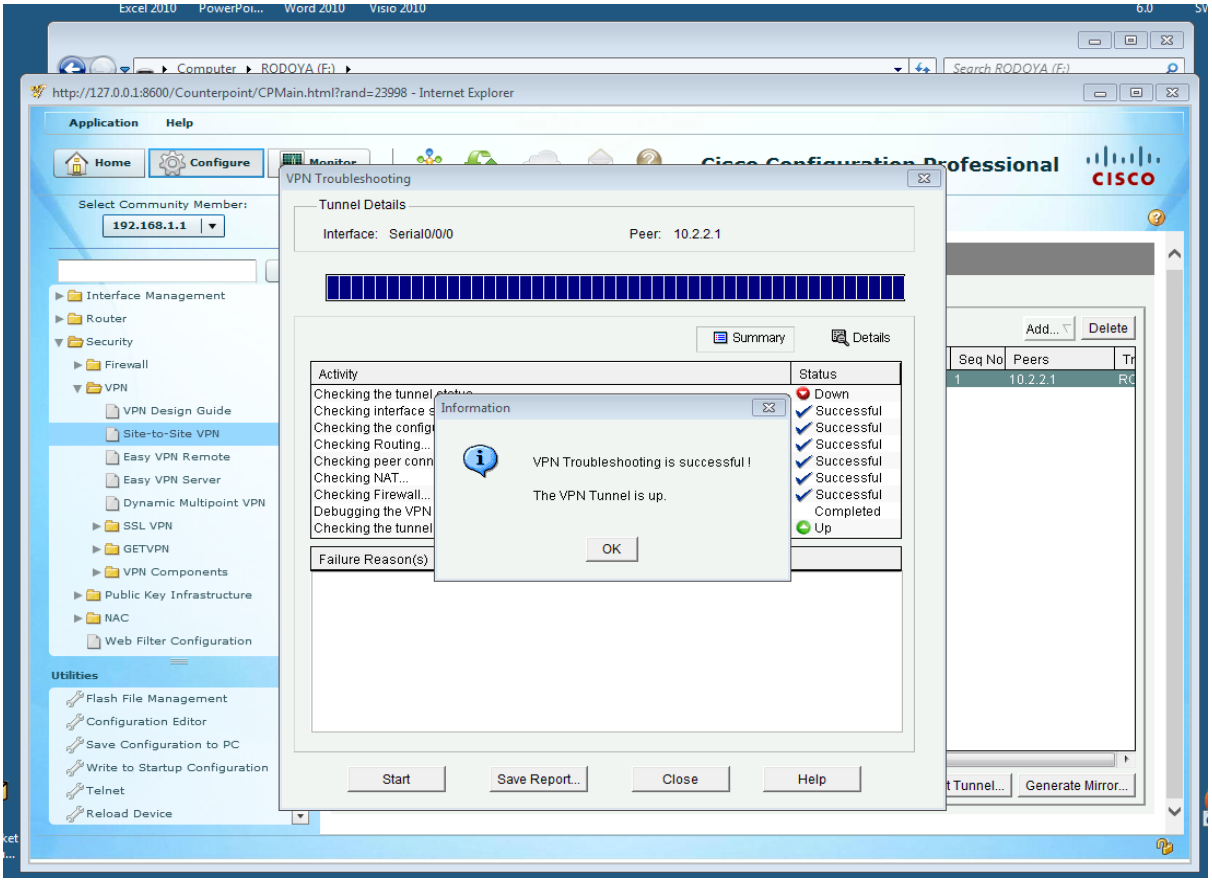


Figure 33.The tunnel details

4.4.2 Testing Result of Remote Access IPSec VPN

In order to check the connectivity we need to have VPN client software on the client side R3. Figure 34 shows how the client software window looks to begin checking a new connection.

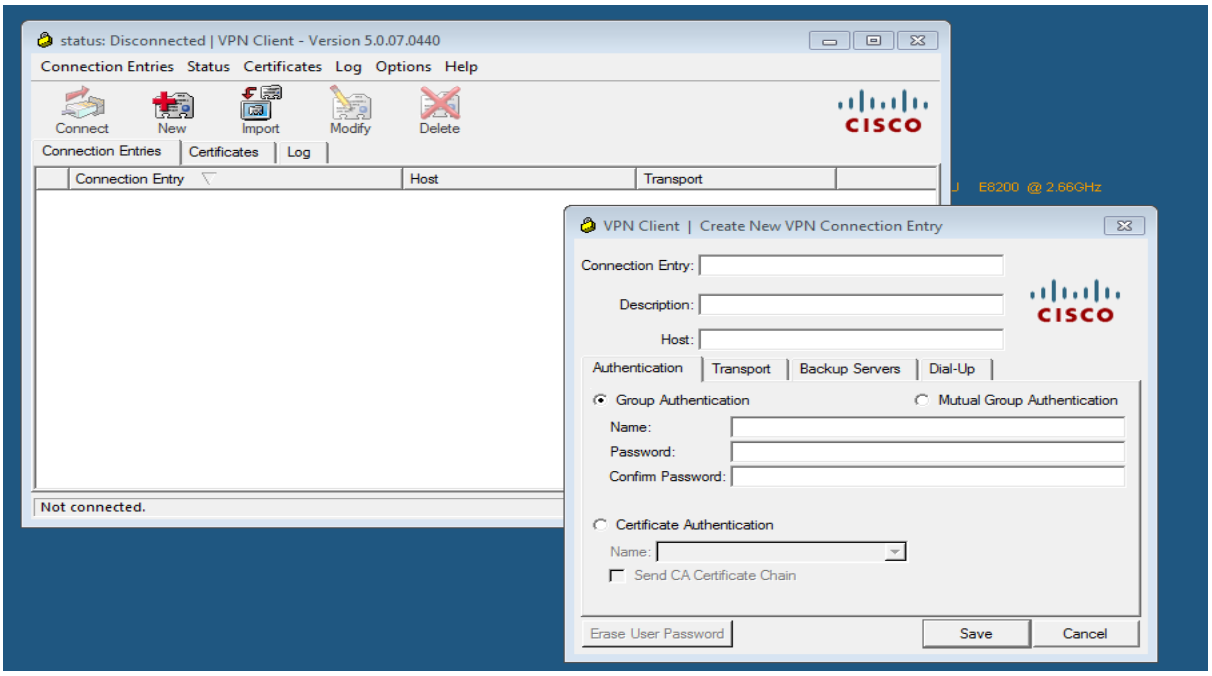


Figure 34.Creating a new VPN entry

Figure 35 below shows the newly connected R1 and it is required to use a user name and password to have the access. We used the right credentials to get in to the server in this step. The user names and passwords are the one used in the above steps.

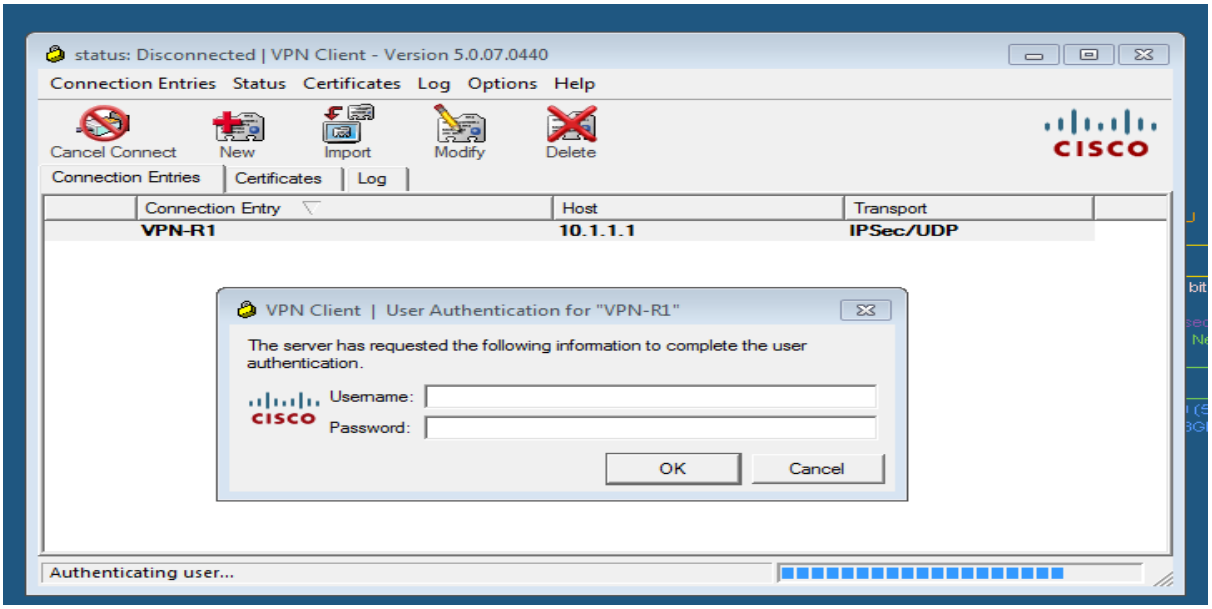


Figure 35.User authentication

Figure 36 shows that the client was connected with main server. The connection was successful and the tunnel was up.

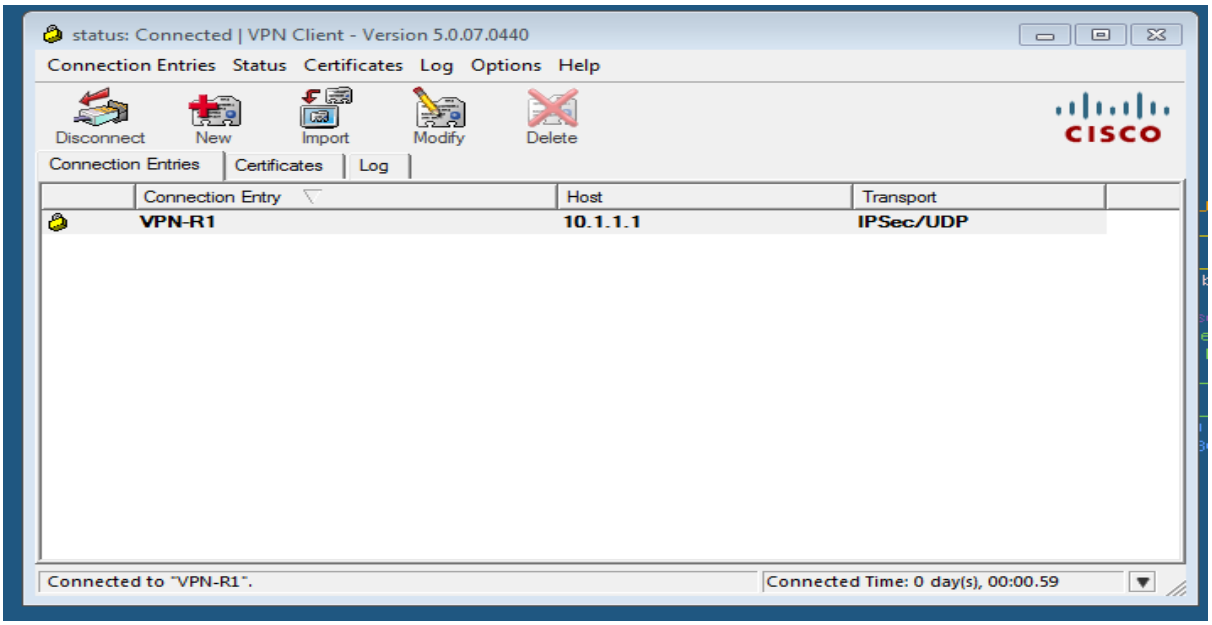


Figure 36.Connected VPN

The window in figure 37 below analysis data related to the created tunnel above. It shows that our servers IP address is 10.1.1.1 .We can get information like encryption and authentication algorithm used, the number of packets encrypted, decrypted, discarded and bypassed.

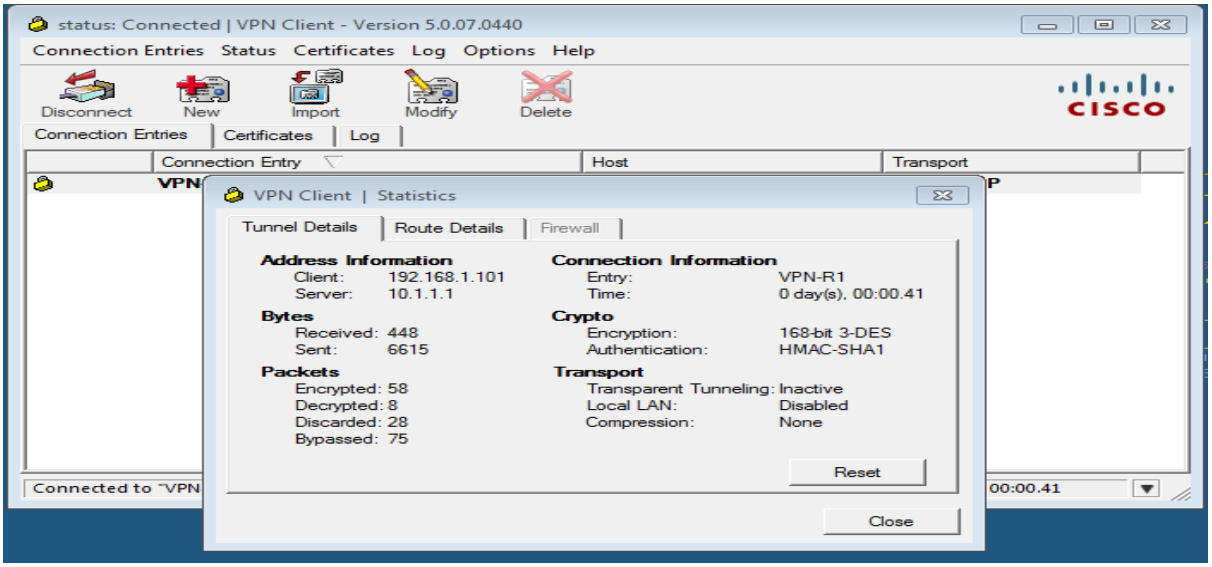


Figure 37.VPN client statistics

The following figure 38 shows the telnet from the clients' cmd. The user admin defined on the configuration was with the higher level that means privilege 15. This makes the prompt as shown on the figure privilege mode R1#.

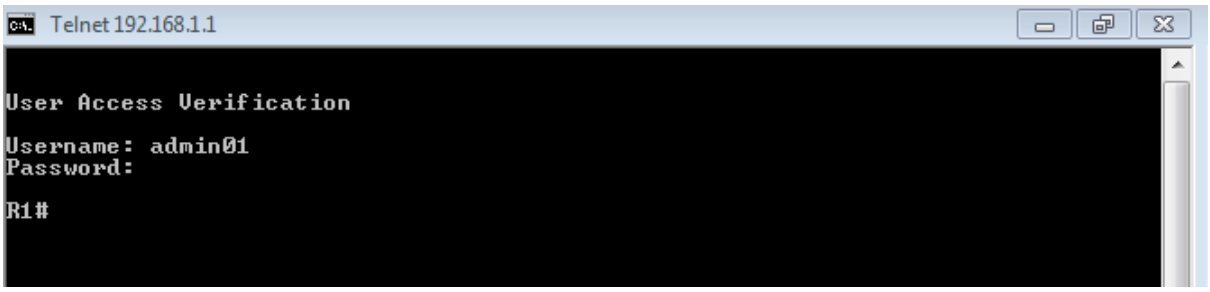


Figure 38.Successful Telnet

Since the VPN connection from the client R3 to the main office is working, the ping both ways should work. The result on figure 39 below shows a ping from cmd line of R3 to 192.168.1.1 and it was successful.

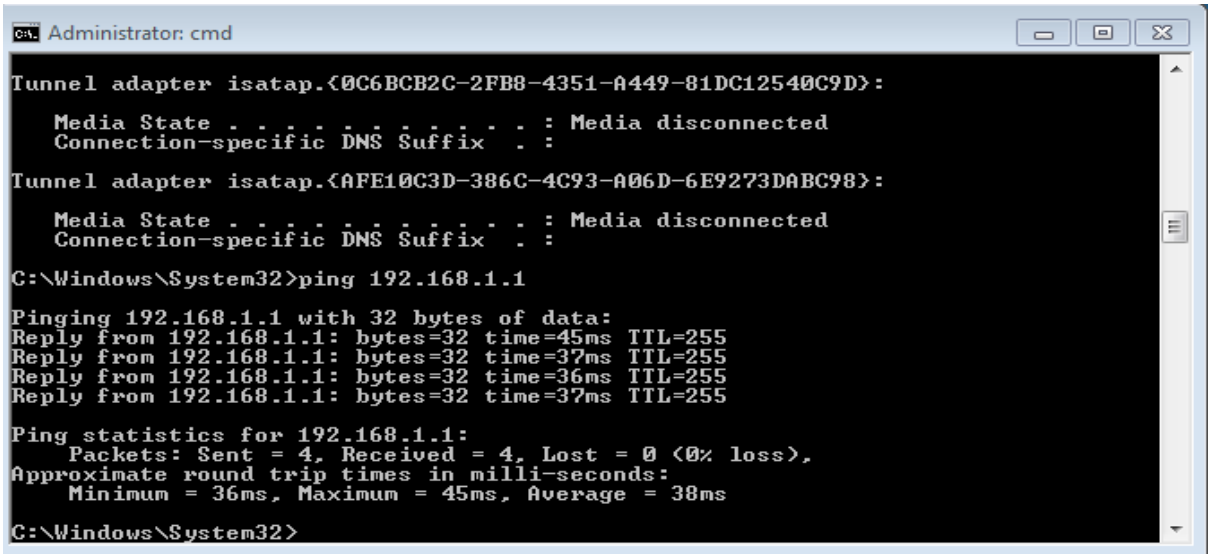


Figure 39.ping 192.168.1.1

The following result in figure 40 demonstrates connection-related data to the client. Some of the formations were IP address, subnet mask and defaults gate way for local area connection and local area connection 2. The IP address, subnet mask and default gateway for local connections are 192.168.3.3, 255.255.255.0, 192.168.3.1. Subsequently, the IP address for local area connection 2 is 192.168.1.101; the subnet mask is 255.255.255.0 and default gateway 192.168.1.1.

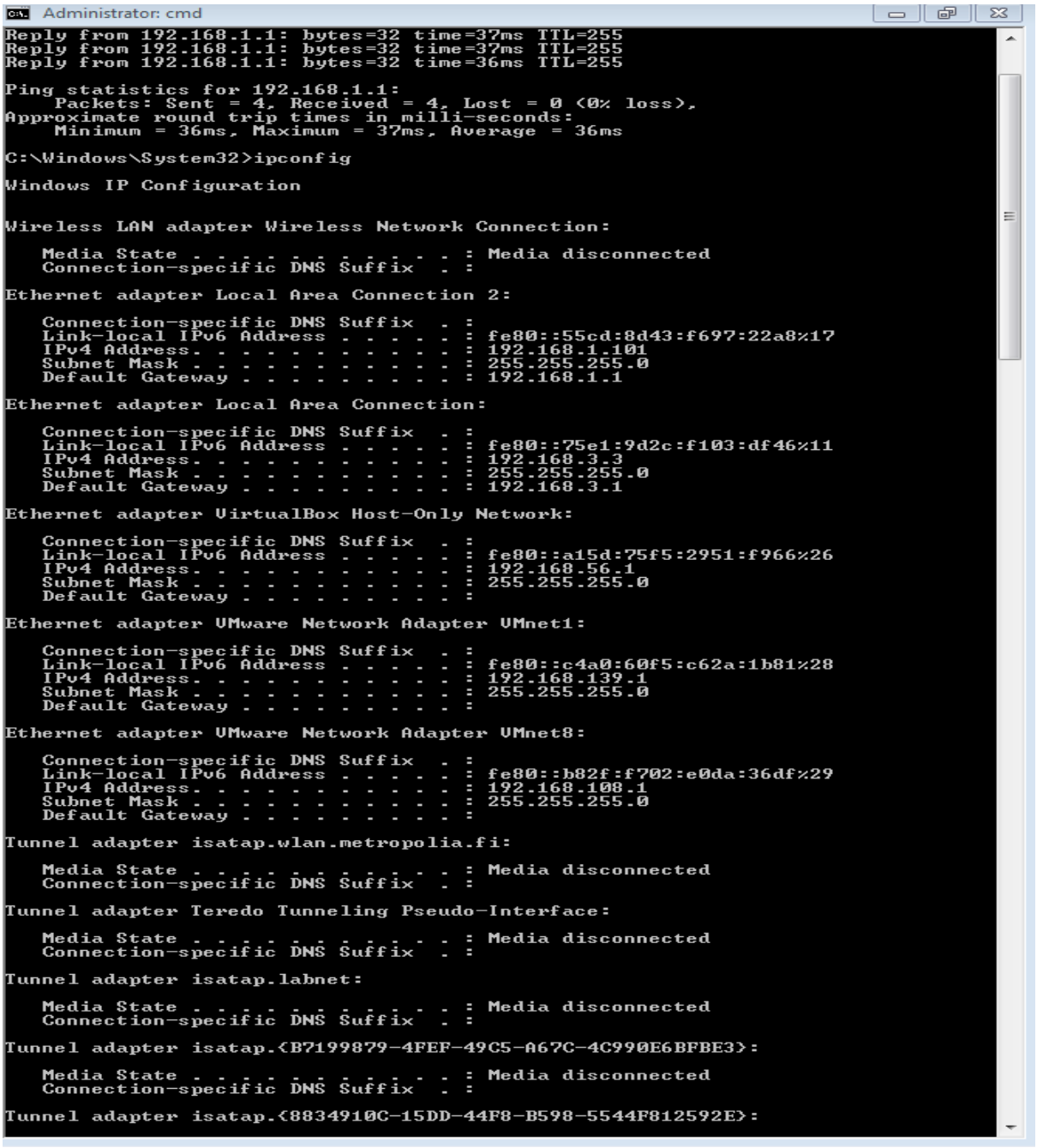


Figure 40.IP configuration on R1

4.4.3 Testing Result of SSL VPN

To test our configuration of SSL I used a web and browsed from the user computer .I launched a web and put the IP address with http://10.1.1.1/ .The windows in the coming windows display the other coming steps. Figure 41 shows successful ping to the main office.

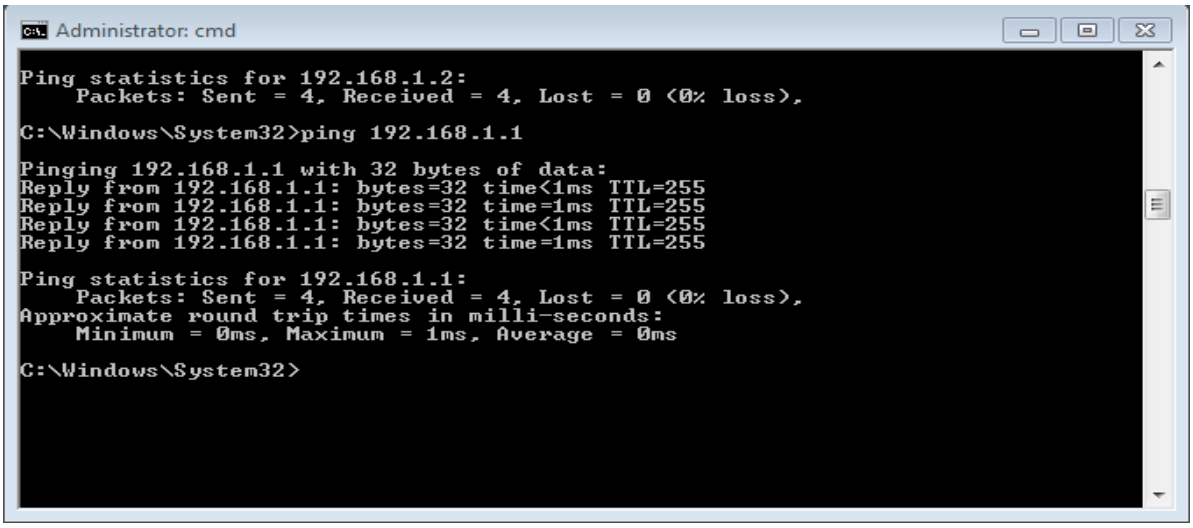


Figure 41.pinging the main office

Figure 42 displays the connection made through the web using http://10.1.1.1/ above. The window displays SSL VPN service requesting the user name and password. The user name I used was adminrodi and password adminrodi123.

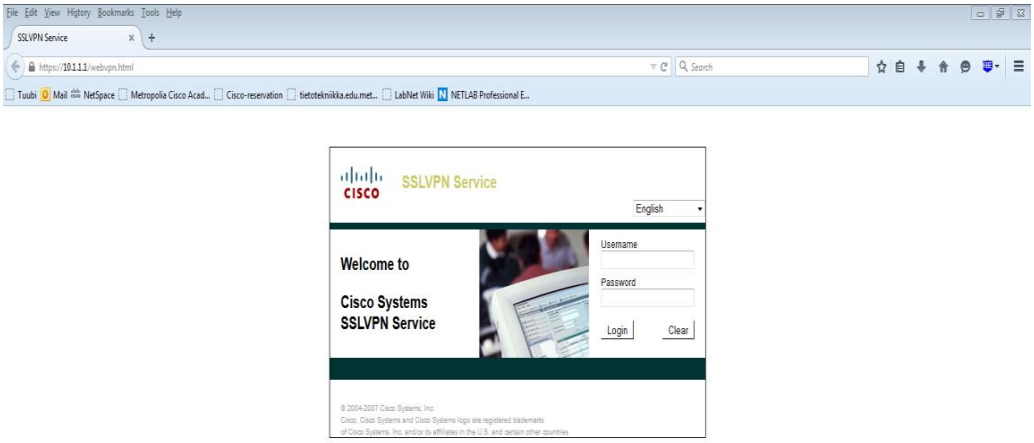


Figure42 .Result from the web using the command http://10.1.1.1

Figure 43 shows the login page and the credentials used for authentication using a user name adminrodi and password adminrodi123.

Figure 43.SSL VPN login

The window in figure 44 displays the login was successful. The employee from the remote office can now access resources of the main office.

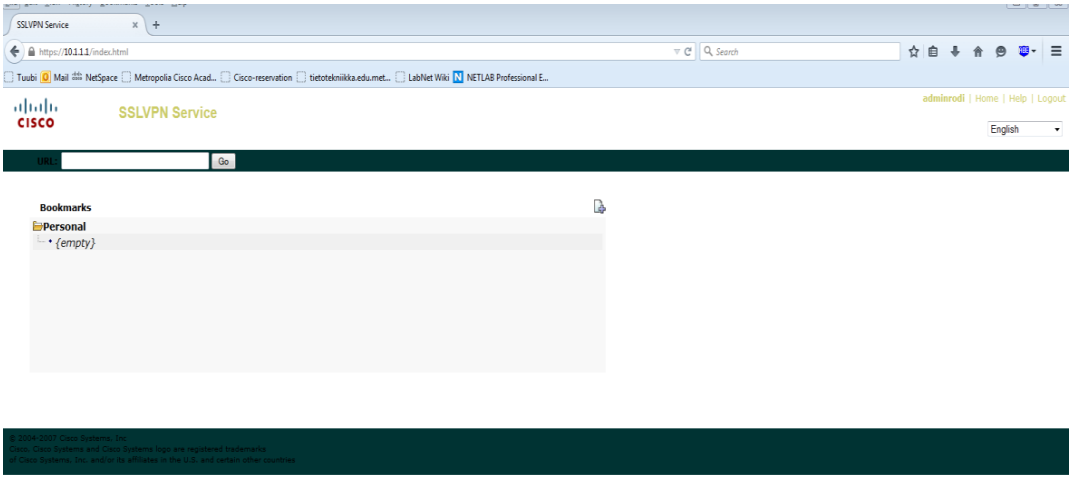


Figure 44. Successful login

5 Conclusions

Currently, companies and network administrators make it a priority to secure their resources and assets by implementing security measures before they offer network-based services. To satisfy this security need, companies have to find the right security solution. When I started the thesis the aim was to create as safe, easily administered and user-friendly a VPN solution as possible. Regarding this, I achieved this objective and learned a great deal about different VPN solutions. Above all, it has been a valuable experience to implement what I have learned practically in the laboratory. The results of the tests were successful and secured to protect the simulated company.

The biggest problems of the current solution are network address translation (NAT) problem and the use of a pre-shared key. Any person with the key can use it as a VPN gateway and other users will have to know the pre-shared key which makes it less secured. NAT is responsible for changing the IP of the internal device to that of NAT device or IKE packet. IKE changes the senders IP address in the packet, and when this new address does not match the original address of the IKE packet, then it will be dropped.

A network security attack is unpredictable. It might occur at any given time and in any location. Therefore, building a reliable security layer on a network system is vital to protect the company from avoidable losses. However, this requires money and time but the benefits outweigh its costs significantly. I conclude that protection of a company's network assets needs a clear security policy that anticipates the types of risks that exit and defend the network. This plan should also describe the measures that need to be taken to stop these losses. The security system should also be monitored constantly to identify inside or outside threats and attacks targeting the company's resources.

I hope and believe that there is a basis for future improvement of this system and with the solutions for authentication and security. The protection of data in terms of confidentiality, availability and integrity needs to be the focal point for future studies and projects.

References

1 Yusuf Bhaiji .Chapter 1: Overview of Network Security. USA: Cisco Press; Jul 25, 2008.
URL: http://www.networkworld.com/article/2274081/lan-wan/chapter-1--overview-of-network security.html
Accessed December 10, 2014.

2 CIPP Guide. CIA triad .UK; August 3rd, 2010.
URL: https://www.cippguide.org/2010/08/03/cia-triad/
Accessed January 5, 2015.

3 Cisco. CCNA security, CCNA Security 640-553 Official course .USA: Cisco press; 2010.

4 Cisco .CCNA security v1.0, Chapter 8.1 Implementing Virtual Private Networks .USA: Ciscopress; April 9, 2009.

5 Chad Perrin. The CIA Triad.USA; June 30, 2008.
URL:http://www.techrepublic.com/blog/it-security/the-cia-triad/.
Accessed January 15, 2015.

6 Elsevier SciTech connects. Defining-a-VPN, chapter 5 Defining-a-VPN. United Kingdom; 2013.
URL: http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Defining-a-VPN.pdf.
Accessed February 6, 2015.

7 Jazib Frahim, Qiang Huan. SSL Remote Access VPN. USA: Cisco Press; June 2008, ISBN: 978-1-58705-242-2, 1-58705-242-3.

8 ETutorials.org. Chapter 7. Virtual Private Network (VPN) Implementation Options
URL:http://etutorials.org/Networking/MPLS+VPN+Architectures/Part+2+MPLS-based+Virtual+Private+Networks/Chapter+7.+Virtual+Private+Network+VPN+Implementation+Options/Overlay+and+Peer-to-peer+VPN+Model/.
Accessed March 2, 2015.

9 Microsoft. TechNet: “what is VPN? “. USA: Microsoft; March 28, 2003.
URL: https://technet.microsoft.com/enus/library/cc739294%28v=ws.10%29.aspx.
Accessed January 12, 2015.

10 Adnan Ahmed Khan, Hassan Zahur. Secure VPN solution in a converged network For Phoniro Systems, AB., an emerging SME. Sweden: September 12, 2012.
URL: http://www.diva-portal.org/smash/get/diva2:559332/FULLTEXT02.pdf.
Accessed January 18, 2015.

11 Simon Baron-Cohen. How is the internet changing the way you think? ;2015

URL: https://edge.org/responses/how-is-the-internet-changing-the-way-you-think.
Accessed February 20, 2015.

12 Karen Scarfone, Paul Hoffman. Guidelines on Firewalls and Firewall Policy.USA: NIST; September, 2009.
URL: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf .
Access on March 7, 2015.

13 Cisco. IPSec VPN WAN Design Overview.USA.
URL:http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html.
Accessed December 2, 2015.

14 AceBit. Explanation of the FTP and SFTP protocols. Germany; 2014.
URL: http://www.wise-ftp.com/know-how/ftp_and_sftp.htm.
Accessed December 6, 2015.

15 Eincopcorporation.GRE (Generic Routing Encapsulation).USA; Saturday, February 21, 2015.
URL: http://blog.eincop.com/2015/02/gre-generic-routing-encapsulation.html .
Accessed March 10, 2015.

16 Cisco. CCNA security, Chapter 8 Lab A, Configuring a Site-to-Site VPN Using Cisco IOS and SDM. USA: Cisco public information; 2010.

17 AllOfVPN Staff.VPN Protocol Comparison.USA; February 2014.
URL: http://allofvpn.com/vpn-protocol-comparison/.
Accessed March 18, 2015.

18 Cisco. Configuring IPSec and ISAKMP .USA.
URL:http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/ike.html.
Accessed April 10, 2015.

Appendix 1: Basic router configuration

```
R1#sh running-config
Building configuration...

Current configuration: 844 bytes
!
Version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
no ip domain-lookup
!
no ip cef
no ipv6 cef
!
no ip domain-lookup
!
Spanning-tree mode pvst
!
Interface FastEthernet0/0
no ip address
duplex auto
speed auto
Shutdown
!
interface FastEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router eigrp 101
network 192.168.1.0
network 10.1.1.0 0.0.0.3
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
ip flow-export version 9
!
security passwords min-length 10
!
no cdp run
!
service password-encryption
!
line con 0
password ciscoconpass
```

```
exec-timeout 0 0
login
logging synchronous

!
line aux 0
!
line vty 0 4
password ciscovtypass
exec-timeout 0 0
login
!
End

copy running-config startup-config

R2#sh running-config
Building configuration...
Current configuration: 901 bytes
!
Version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
no ip cef
no ipv6 cef
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.252
clock rate 64000
!
interface Vlan1
no ip address
shutdown
!
security passwords min-length 10
!
router eigrp 101
network 10.1.1.0 0.0.0.3
network 10.2.2.0 0.0.0.3
no auto-summary
!
```

```
ip classless
ip route 192.168.1.0 255.255.255.0 10.1.1.1
ip route 192.168.3.0 255.255.255.0 10.2.2.1
!
ip flow-export version 9
!
service password-encryption
!

no cdp run
!
line con 0
password ciscoconpass
exec-timeout 0 0
login
logging synchronous
!
line aux 0
!
line vty 0 4
password ciscovtypass
exec-timeout 0 0
login
!
end
copy running-config startup-config

R3#sh running-config
Building configuration...

Current configuration : 824 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
no ip cef
no ipv6 cef
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
ip address 192.168.3.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
!
```

```
interface Vlan1
no ip address
shutdown
!
router eigrp 101
network 192.168.3.0
network 10.2.2.0 0.0.0.3
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
ip flow-export version 9
!
security passwords min-length 10
!
no cdp run
!
service password-encryption
!
line con 0
password ciscoconpass
exec-timeout 0 0
login
logging synchronous
line aux 0
!
line vty 0 4
password ciscovtypass
exec-timeout 0 0
login
end
copy running-config startup-config
```

Appendix 2: Mirror configuration for site-to-site –R3

```
crypto isakmp policy 10
 authentication pre-share
 encr aes 256
 hash md5
 group 5
 lifetime 86400
 exit
crypto isakmp key cisco12345 address 10.1.1.1
crypto ipsec transform-set RODOYAThesis esp-sha-hmac esp-aes 256
 mode tunnel
 exit
ip access-list extended SDM_1
 remark CCP_ACL Category=4
 remark IPSec Rule
 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
 exit
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Apply the crypto map on the peer router's interface having IP
address 10.2.2.1 that connects to this router.
 set transform-set RODOYAThesis
 set peer 10.1.1.1
 match address SDM_1
 exit
```

Appendix 3: Site to site configuration for R1

```
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
no logging buffered
!
no aaa new-model
!
memory-size iomem 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-493412598
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-493412598
 revocation-check none
 rsakeypair TP-self-signed-493412598
!
crypto pki certificate chain TP-self-signed-493412598
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 34393334 31323539 38301E17 0D313530 33323330 38333435
  375A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3439 33343132
  35393830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  B19C1DA5 BFC4EB47 8D76F52F A7894E66 75EF0268 C4196A59 68B3638D 359929A7
  1CF52618 B5ECA88D 8B39C1DF BAABBD55 5B76FB34 CC2B7188 8FA9B4CE 2C90BCAF
  1E89E913 212A7AEF AEE3E93F 67E6AE80 EC006319 E26F68F6 360BA1F1 035D605C
  8609FA39 9E6F0E89 FC98DE3C A3277C29 A5903632 82311E28 9E722629 9C9E057B
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
  23041830 168014EC 49E56CFC F45FF7C7 7CDC70CB 5FD45831 C34C9230 1D060355
  1D0E0416 0414EC49 E56CFCF4 5FF7C77C DC70CB5F D45831C3 4C92300D 06092A86
  4886F70D 01010505 00038181 00585A8F F4B96DC9 3C8D4062 B20F1CCF 56561A29
  D5BB32EE 3ED2067E 2F3038DD 42B086E7 D11CC8DF B39D93A6 3E7594DA CE4EE799
  D4F8B515 4D25724F 87945937 8E953624 36332FBB A01AFA1D 61C3BB2E FFE3255B
  5F3DB1B2 6CB42351 C0C86344 0A9E1664 9D9C26A2 1AEBA7BF 95882D34 2A4AADA7
  6F98162F 36975632 26A9EDE0 52
        quit
!
license udi pid CISCO2811 sn FCZ133770S6
vtp domain TSHOOT
vtp mode transparent
username admin privilege 15 secret 5 $1$7ALU$KDmFkuHu86Tin7prH86141
!
redundancy
!
crypto isakmp policy 1
```

```
 encr 3des
 authentication pre-share
group 2
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key cisco12345 address 10.2.2.1
!
crypto ipsec transform-set RODOYAThesis esp-aes 256 esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to10.2.2.1
 set peer 10.2.2.1
 set transform-set RODOYAThesis
 match address 100
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 no fair-queue
 clock rate 2000000
 crypto map SDM_CMAP_1
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router eigrp 101
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip flow-export version 9
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
access-list 100 remark CCP_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
no cdp run
!
control-plane
!
mgcp profile default
!
line con 0
 exec-timeout 0 0
```

```
 password 7 05080F1C22434D061715160118
 logging synchronous
 login
line aux 0
line vty 0 4
 exec-timeout 0 0
 password 7 00071A1507541D1216314D5D1A
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

Appendix 4: Site to site configuration for R3

```
hostname R3
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
!
no aaa new-model
!
memory-size iomem 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1429020141
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1429020141
 revocation-check none
 rsakeypair TP-self-signed-1429020141
!
crypto pki certificate chain TP-self-signed-1429020141
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31343239 30323031 3431301E 170D3135 30333233 31303037
  30315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 34323930
  32303134 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100A467 4D4901D7 E1AE6D4D 746EE101 BF62F577 4188F308 E5245F70 9D3E9B6A
  B955DE68 BAF488B5 B4F16BC6 44122C3E EE1B7782 12F7FC52 07339688 B73BD6B7
  CB5D0A0A 524035F3 73C347AC E7B9E3BD 503E6256 FBB6E585 D54C791E C5F1A89F
  B08D0CA7 497DFCA5 93AF96CC 76025D24 631A242B DCDF4E1B BF20D3AC DA8626D4
  B41B0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 1466B5A7 13E2D202 AE857978 55E21914 76C82581 59301D06
  03551D0E 04160414 66B5A713 E2D202AE 85797855 E2191476 C8258159 300D0609
  2A864886 F70D0101 05050003 8181004E F4BD70AA A6410BF1 482949B3 B1350DD3
  2781908B 5E21D2A6 74F1F23A 3B21C9FD C78943BF 13F9432A C587A1FF D46208DB
  ACB8B958 AC08BB24 73186F93 D26B588A 68C13753 C3F2AB93 FF9DD811 4E430BC6
  EA7E1D3D 4A631968 FF70C6CF 0C90682A 7925EBBB 17E5FA06 59AA9877 51492D51
  9CF3F813 FB454EEF 19053308 C70440
        quit
!
license udi pid CISCO2811 sn FCZ133770RU
username admin privilege 15 secret 5 $1$hzqJ$Rk3irZD3SJwCPpRd0hPep0
!
redundancy
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
```

```
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key cisco12345 address 10.1.1.1
!
crypto ipsec transform-set RODOYAThesis esp-aes 256 esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Apply the crypto map on the peer router's interface having IP
address 10.2.2.1 that connects to this router.
 set peer 10.1.1.1
 set transform-set RODOYAThesis
 match address SDM_1
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 crypto map SDM_CMAP_1
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router eigrp 101
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip flow-export version 9
!
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
ip access-list extended SDM_1
 remark CCP_ACL Category=4
 remark IPSec Rule
 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
!
```

```
no cdp run
!
control-plane
!
mgcp profile default
!
line con 0
 exec-timeout 0 0
 password 7 121A0C0411040F0B243B253B20
 logging synchronous
 login
line aux 0
line vty 0 4
 exec-timeout 0 0
 password 7 02050D4808091935555E080A16
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

Appendix 5: Remote access configuration for R1

```
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
!
aaa new-model
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
aaa authorization network ciscocp_vpn_group_ml_1 local
!
aaa session-id common
!
memory-size iomem 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-493412598
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-493412598
 revocation-check none
 rsakeypair TP-self-signed-493412598
!
crypto pki certificate chain TP-self-signed-493412598
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 34393334 31323539 38301E17 0D313530 33323331 31323135
  335A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3439 33343132
  35393830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  A2C43988 1E85B10D 604B6F7D 7A5FCC9F 809F3E31 1D04AD0B 4C5FEAF4 6C2092A2
  A6D238EF 987C0E29 53EBF66F ADA6FBE9 E87FA979 62E35533 F5A47163 FACBECDF
  503BA730 90B920B3 222AF8FA B3455035 A5370B84 DE710DAE A3BD2687 B51F1A7A
  328E23BE 3D2D1230 98F1D10F 3C09690C 0930E363 58F81686 A0A379EF 6DA8465F
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
  23041830 168014FF 3DF0CDAD E1A4E18C 9234DACF 4C92CBE4 C3066930 1D060355
  1D0E0416 0414FF3D F0CDADE1 A4E18C92 34DACF4C 92CBE4C3 0669300D 06092A86
  4886F70D 01010505 00038181 00872FA9 5BD1F257 D4C4ACDC 90F54149 85DF0C7B
  0692D1D3 C7779751 6C506805 7EF738A0 810D916F 4701DDAC 9A65656D BD3A2264
  F4558DF0 64AB58EF BDF9E372 293C7365 FE1517FF DE1D23F5 E3DCB1C6 5C51A4F8
  0A74F057 763CF02E EF6816F3 CAE5E726 F0C5C4B2 D9F2B38A DE73CFCC AA22ED04
  0DEEC29E 90F6F138 25DCE23C C9
        quit
!
license udi pid CISCO2811 sn FCZ133770S6
vtp domain TSHOOT
```

```
vtp mode transparent
username admin01 privilege 15 password 7 050A020228421E5809040401
username rodi01 privilege 15 password 7 00161C020D0B5A070C22495D1A
username VPNuser1 secret 5 $1$Zi5.$wq6J9MKjoMyI3btLocjOR/
!
redundancy
!
class-map type inspect match-any SDM_AH
 match access-group name SDM_AH
class-map type inspect match-any ccp-skinny-inspect
 match protocol skinny
class-map type inspect match-any ccp-cls-insp-traffic
 match protocol dns
 match protocol ftp
 match protocol https
 match protocol icmp
 match protocol imap
 match protocol pop3
 match protocol netshow
 match protocol shell
 match protocol realmedia
 match protocol rtsp
 match protocol smtp
 match protocol sql-net
 match protocol streamworks
 match protocol tftp
 match protocol vdolive
 match protocol tcp
 match protocol udp
class-map type inspect match-all ccp-insp-traffic
 match class-map ccp-cls-insp-traffic
class-map type inspect match-any SDM_IP
 match access-group name SDM_IP
class-map type inspect match-any SDM_ESP
 match access-group name SDM_ESP
class-map type inspect match-any SDM_EASY_VPN_SERVER_TRAFFIC
 match protocol isakmp
 match protocol ipsec-msft
 match class-map SDM_AH
 match class-map SDM_ESP
class-map type inspect match-all SDM_EASY_VPN_SERVER_PT
 match class-map SDM_EASY_VPN_SERVER_TRAFFIC
class-map type inspect match-any ccp-h323nxg-inspect
 match protocol h323-nxg
class-map type inspect match-any ccp-cls-icmp-access
 match protocol icmp
 match protocol tcp
 match protocol udp
class-map type inspect match-any ccp-h225ras-inspect
 match protocol h225ras
class-map type inspect match-any ccp-h323annexe-inspect
 match protocol h323-annexe
class-map type inspect match-any ccp-h323-inspect
 match protocol h323
class-map type inspect match-all ccp-invalid-src
 match access-group 100
class-map type inspect match-all ccp-icmp-access
 match class-map ccp-cls-icmp-access
class-map type inspect match-any ccp-sip-inspect
 match protocol sip
class-map type inspect match-all ccp-protocol-http
 match protocol http
!
policy-map type inspect ccp-permit-icmpreply
 class type inspect ccp-icmp-access
```

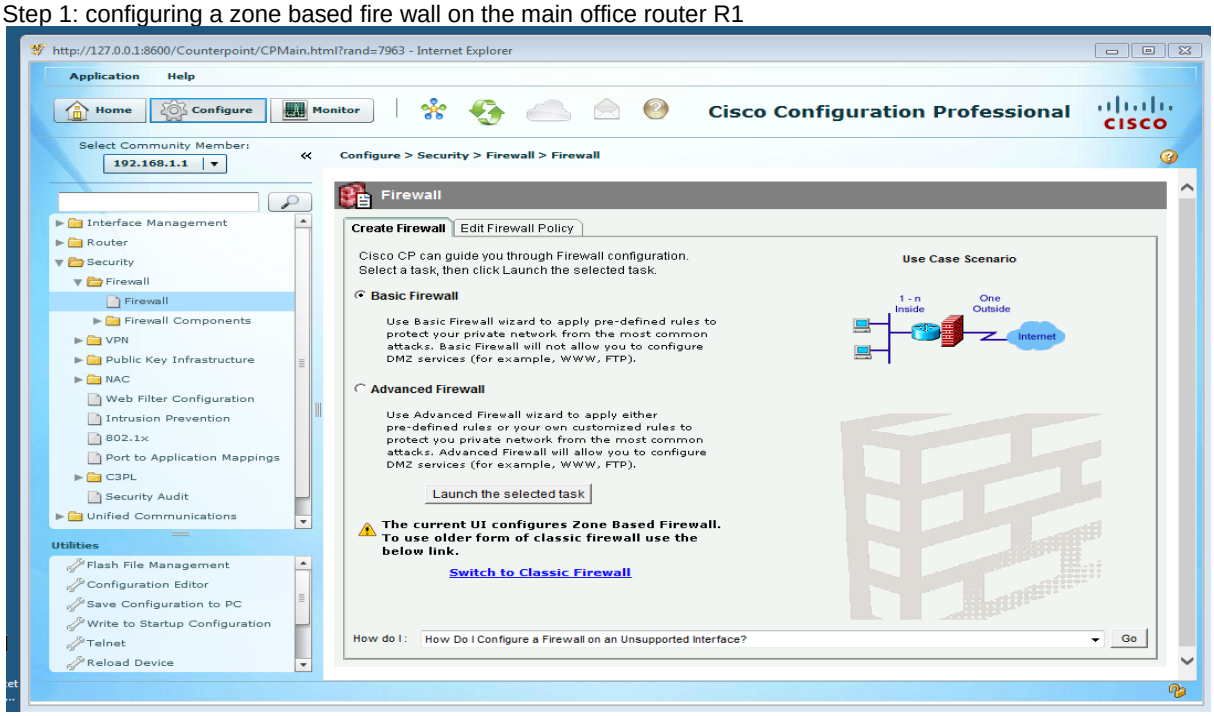
```
  inspect
 class type inspect ccp-sip-inspect
  inspect
 class type inspect ccp-h323-inspect
  inspect
 class type inspect ccp-h323annexe-inspect
  inspect
 class type inspect ccp-h225ras-inspect
  inspect
 class type inspect ccp-h323nxg-inspect
  inspect
 class type inspect ccp-skinny-inspect
  inspect
 class class-default
  pass
policy-map type inspect ccp-inspect
 class type inspect ccp-invalid-src
  drop log
 class type inspect ccp-protocol-http
  inspect
 class type inspect ccp-insp-traffic
  inspect
 class type inspect ccp-sip-inspect
  inspect
 class type inspect ccp-h323-inspect
  inspect
 class type inspect ccp-h323annexe-inspect
  inspect
 class type inspect ccp-h225ras-inspect
  inspect
 class type inspect ccp-h323nxg-inspect
  inspect
 class type inspect ccp-skinny-inspect
  inspect
 class class-default
  drop
policy-map type inspect ccp-permit
 class type inspect SDM_EASY_VPN_SERVER_PT
  pass
 class type inspect ccp-sip-inspect
  inspect
 class type inspect ccp-h323-inspect
  inspect
 class type inspect ccp-h323annexe-inspect
  inspect
 class type inspect ccp-h225ras-inspect
  inspect
 class type inspect ccp-h323nxg-inspect
  inspect
 class type inspect ccp-skinny-inspect
  inspect
 class class-default
  drop
policy-map type inspect sdm-permit-ip
 class type inspect SDM_IP
  pass
 class class-default
  drop log
!
zone security in-zone
zone security out-zone
zone security ezvpn-zone
zone-pair security ccp-zp-self-out source self destination out-zone
 service-policy type inspect ccp-permit-icmpreply
zone-pair security ccp-zp-in-out source in-zone destination out-zone
```

```
 service-policy type inspect ccp-inspect
zone-pair security ccp-zp-out-self source out-zone destination self
 service-policy type inspect ccp-permit
zone-pair security sdm-zp-in-ezvpn1 source in-zone destination ezvpn-zone
 service-policy type inspect sdm-permit-ip
zone-pair security sdm-zp-out-ezpn1 source out-zone destination ezvpn-zone
 service-policy type inspect sdm-permit-ip
zone-pair security sdm-zp-ezvpn-out1 source ezvpn-zone destination out-zone
 service-policy type inspect sdm-permit-ip
zone-pair security sdm-zp-ezvpn-in1 source ezvpn-zone destination in-zone
 service-policy type inspect sdm-permit-ip
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group ROD-access
 key RODaccess12345
 pool SDM_POOL_1
 max-users 100
 netmask 255.255.255.0
crypto isakmp profile ciscocp-ike-profile-1
   match identity group ROD-access
   client authentication list ciscocp_vpn_xauth_ml_1
   isakmp authorization list ciscocp_vpn_group_ml_1
   client configuration address respond
   virtual-template 1
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto ipsec profile CiscoCP_Profile1
 set security-association idle-time 900
 set transform-set ESP-3DES-SHA
 set isakmp-profile ciscocp-ike-profile-1
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description $FW_INSIDE$
 ip address 192.168.1.1 255.255.255.0
 zone-member security in-zone
 duplex auto
 speed auto
!
interface Serial0/0/0
 description $FW_OUTSIDE$
 ip address 10.1.1.1 255.255.255.252
 zone-member security out-zone
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Virtual-Template1 type tunnel
 ip unnumbered Serial0/0/0
 zone-member security ezvpn-zone
 tunnel mode ipsec ipv4
```

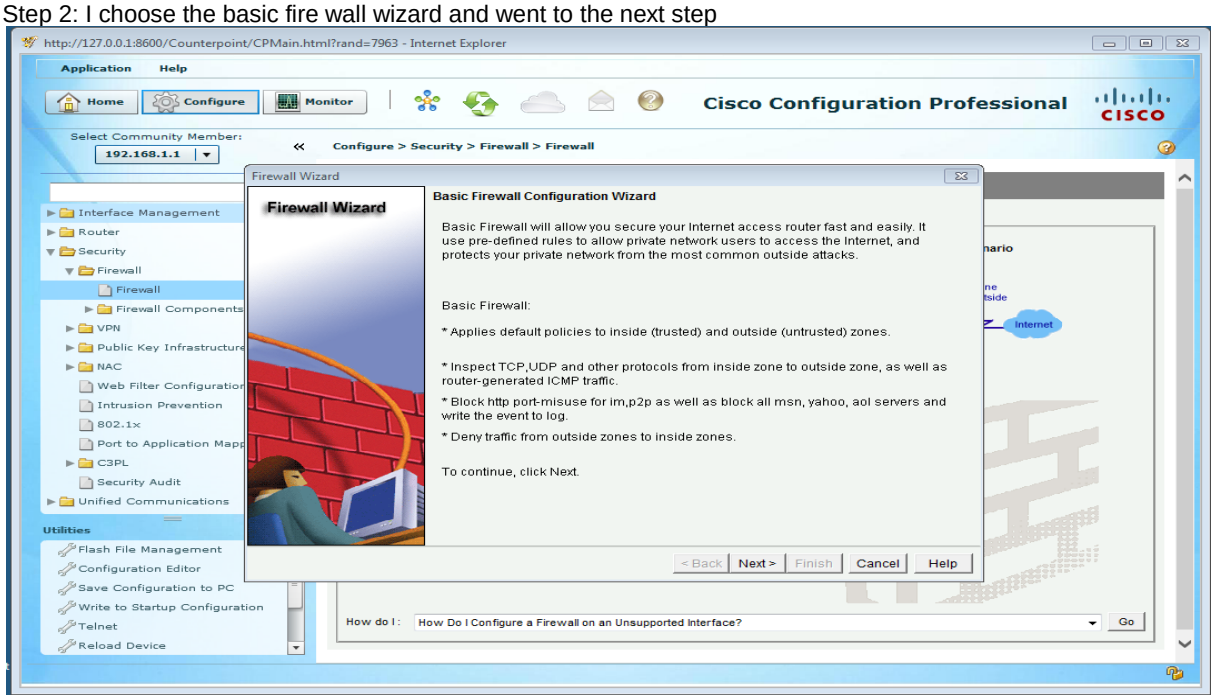
```
 tunnel protection ipsec profile CiscoCP_Profile1
!
ip local pool SDM_POOL_1 192.168.1.100 192.168.1.150
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip flow-export version 9
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
ip access-list extended SDM_AH
 remark CCP_ACL Category=1
 permit ahp any any
ip access-list extended SDM_ESP
 remark CCP_ACL Category=1
 permit esp any any
ip access-list extended SDM_IP
 remark CCP_ACL Category=1
 permit ip any any
!
access-list 100 remark CCP_ACL Category=128
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip 10.1.1.0 0.0.0.3 any
no cdp run
!
control-plane
!
mgcp profile default
!
line con 0
 exec-timeout 0 0
 password 7 030752180500224340191816O4
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 0 0
 password 7 045802150C2E5A5A1009040401
 transport input all
!
scheduler allocate 20000 1000
end
```

Appendix 6: Remote access configuration

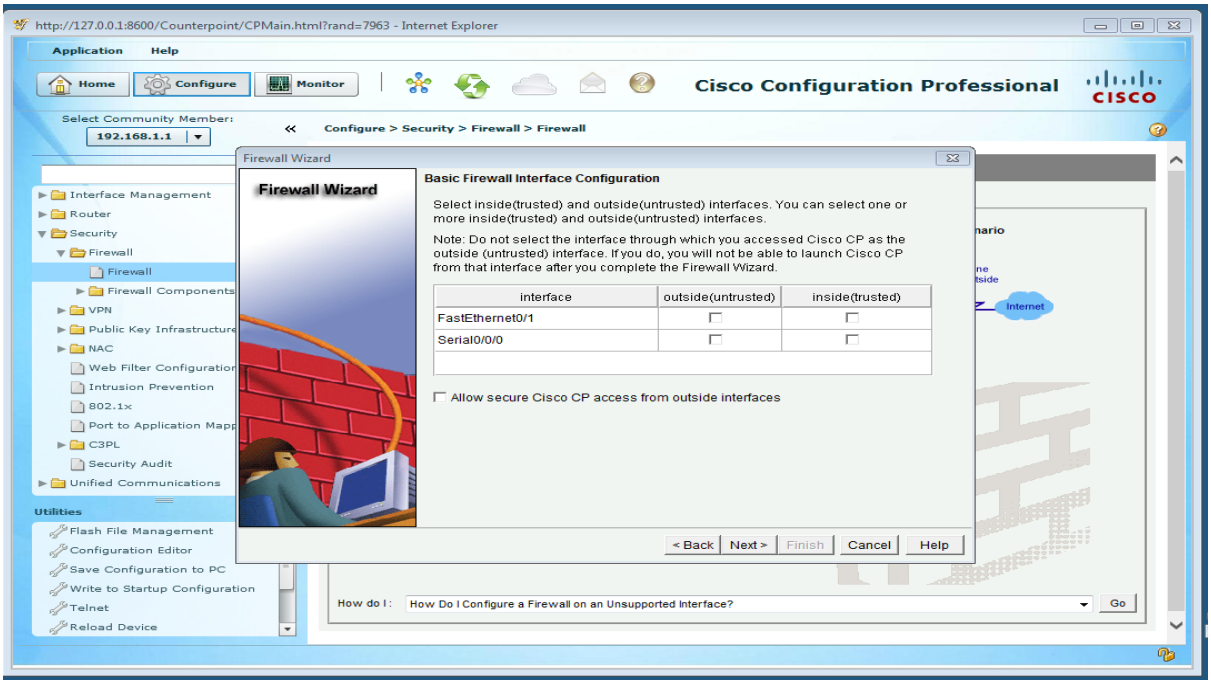
Step 1: configuring a zone based fire wall on the main office router R1



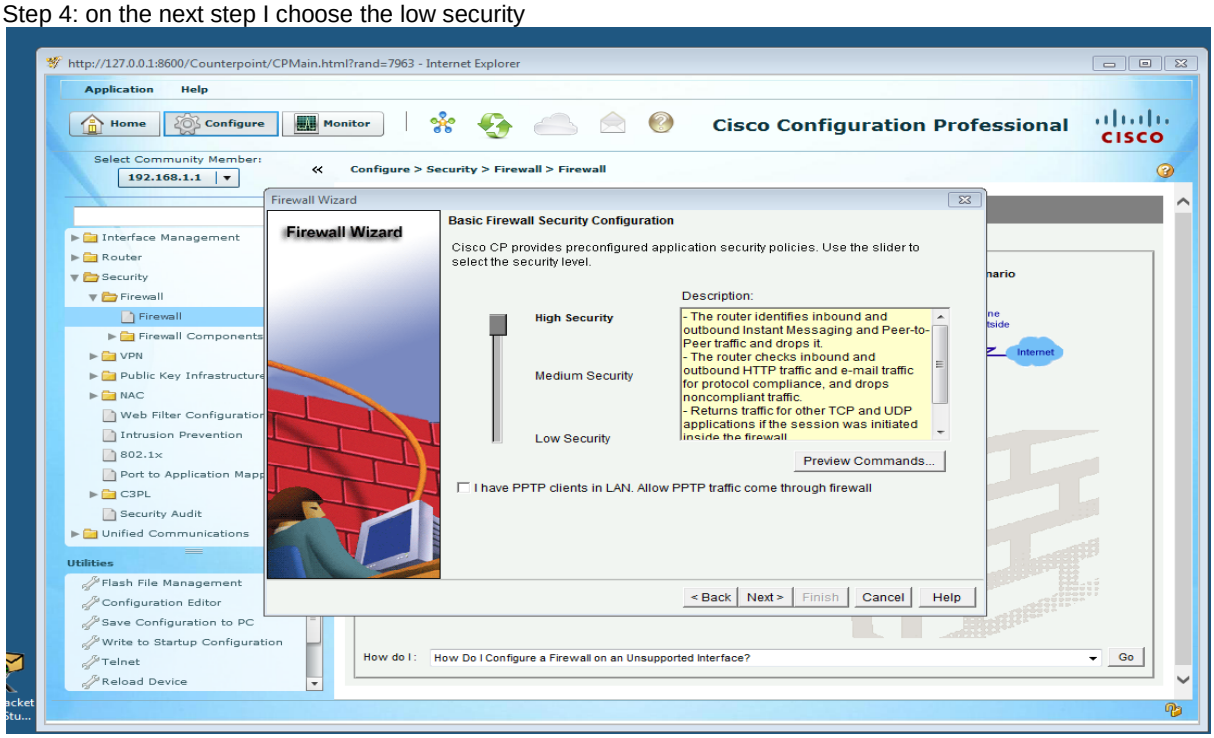
Step 2: I choose the basic fire wall wizard and went to the next step



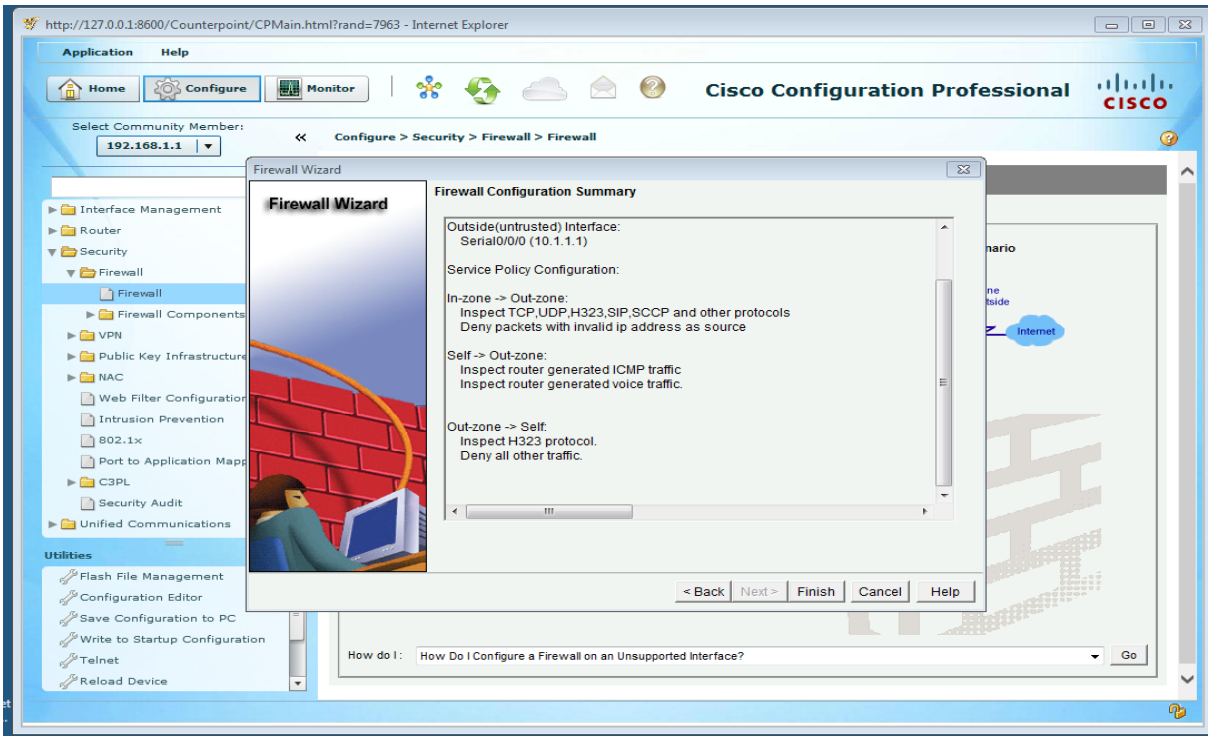
Step 3: on the next step I choose to check the fast Ethernet 0/1 for inside and outside for the serial 0/0/0



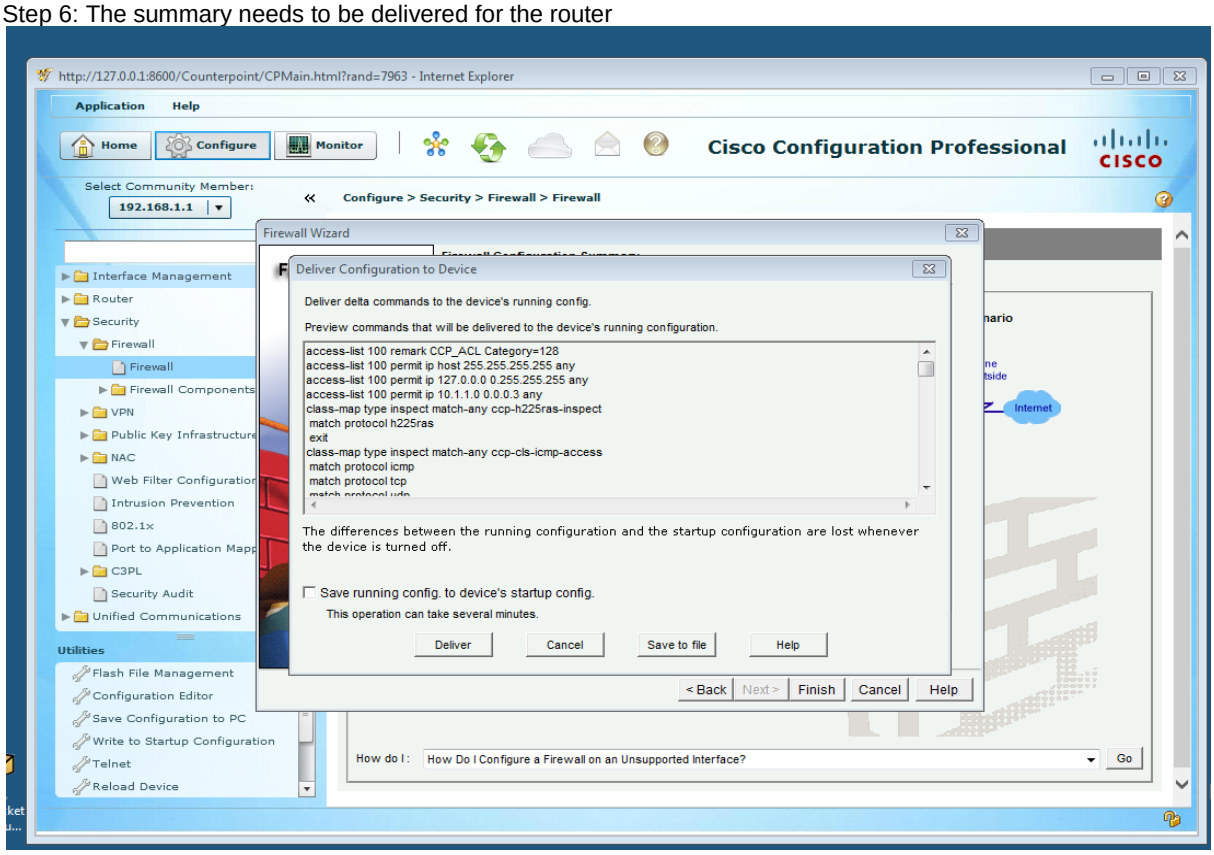
Step 4: on the next step I choose the low security



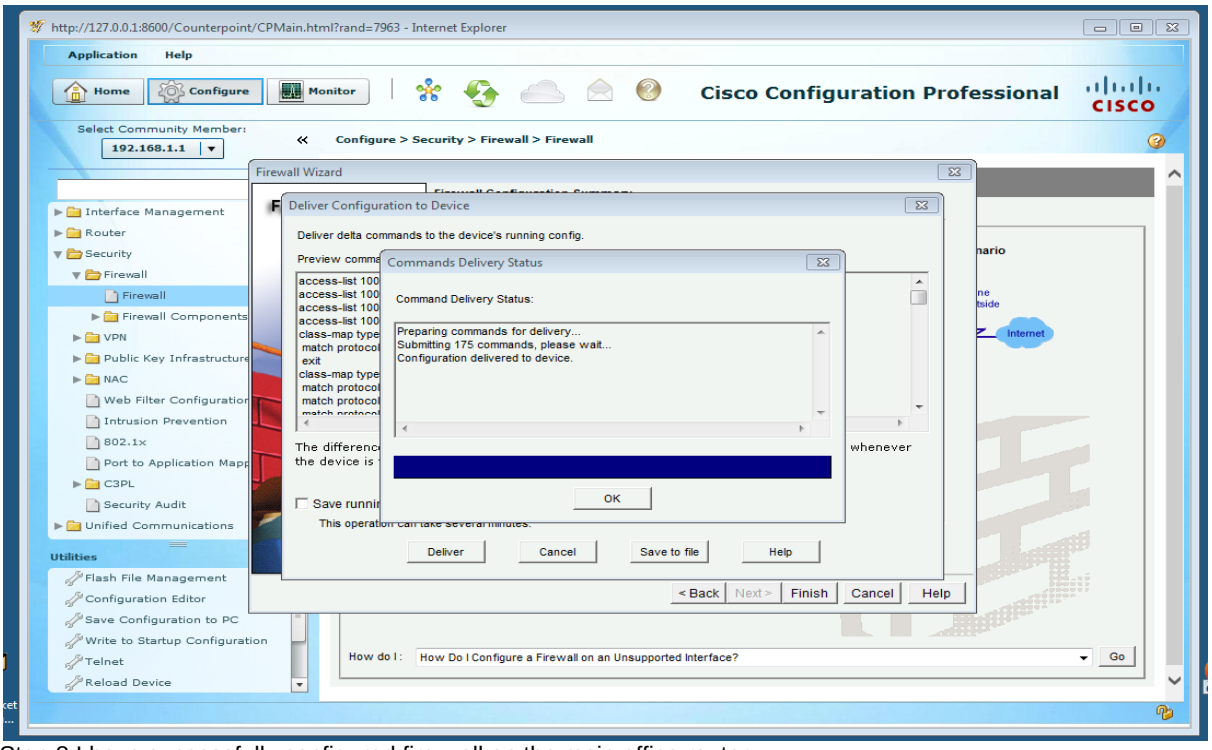
Step 5: Then fire wall configuration comes and finished



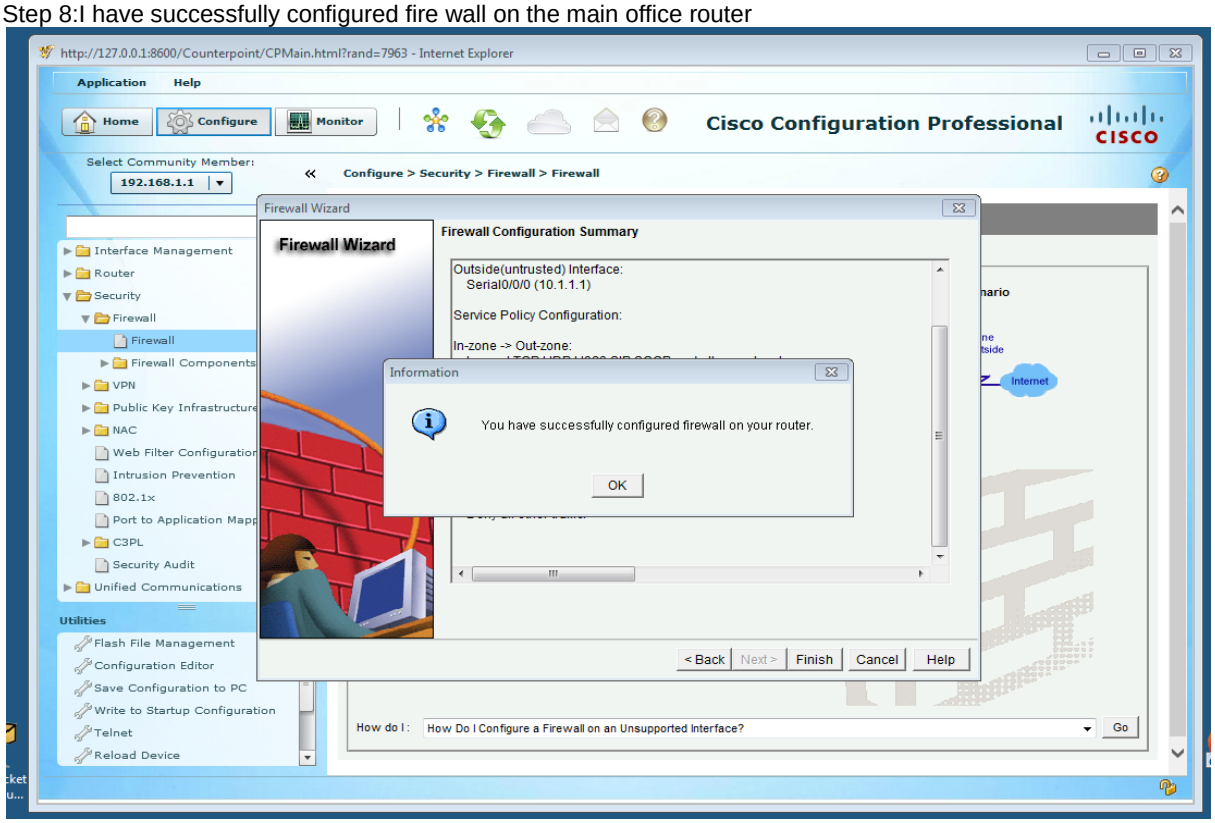
Step 6: The summary needs to be delivered for the router



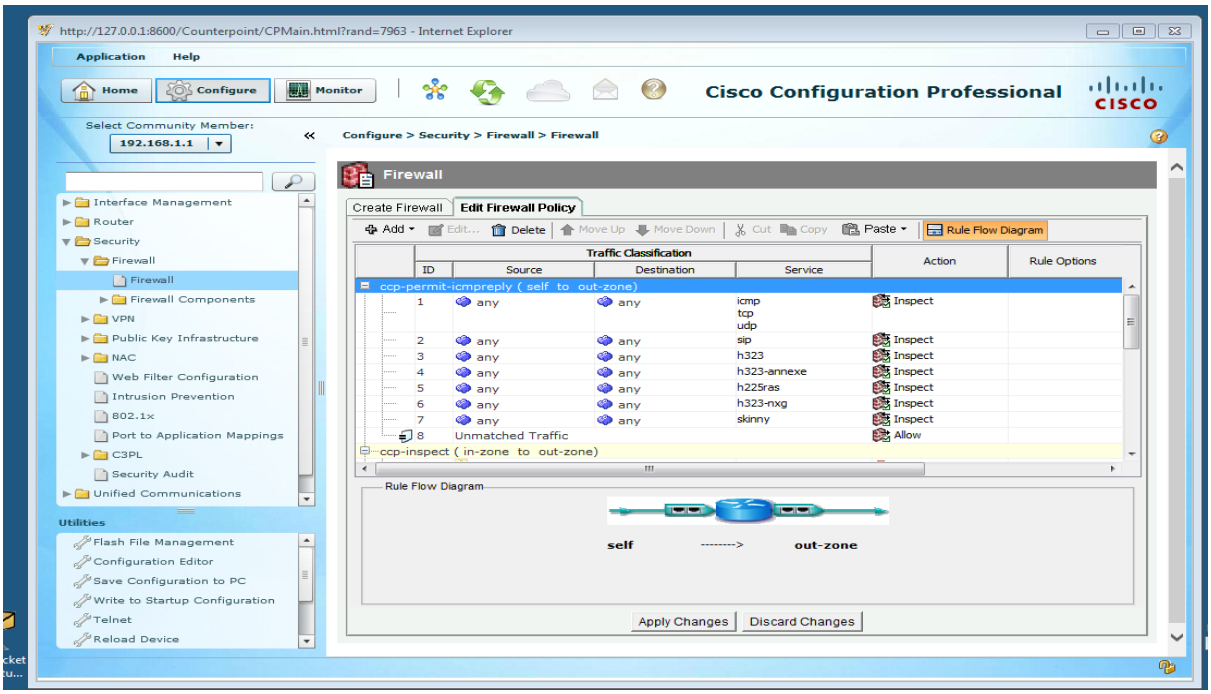
Step 7: The following screen shows the status for the delivery to the router



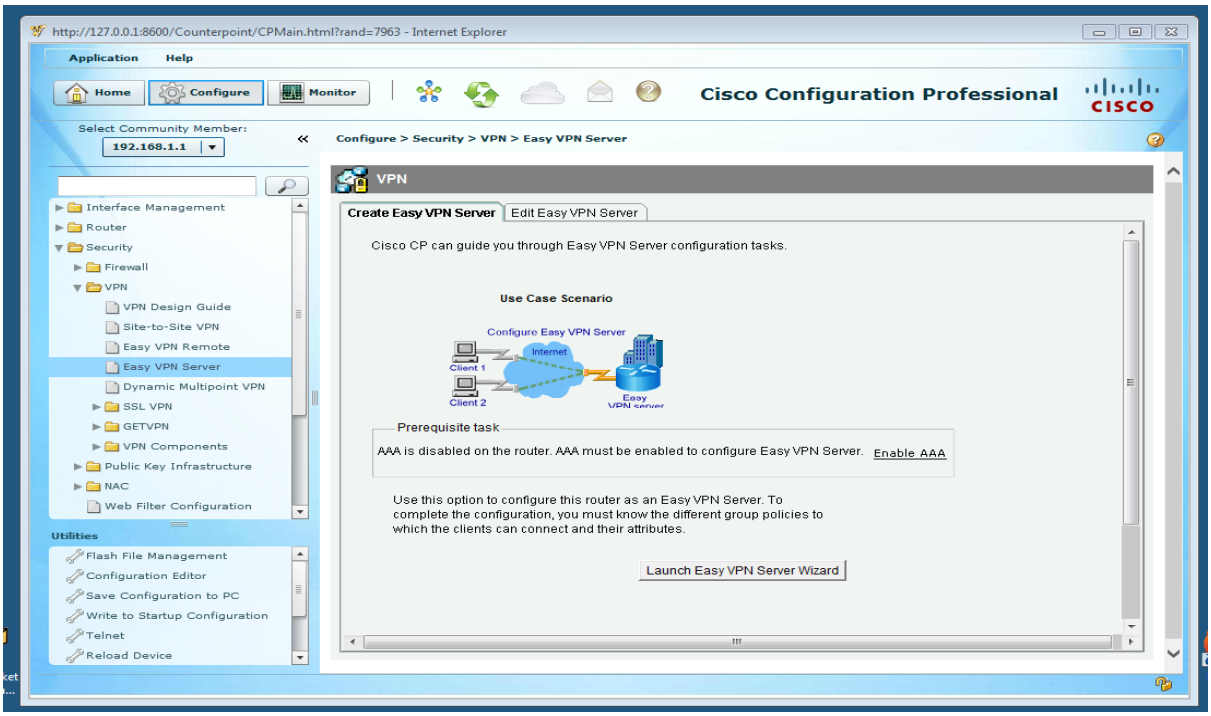
Step 8:I have successfully configured fire wall on the main office router



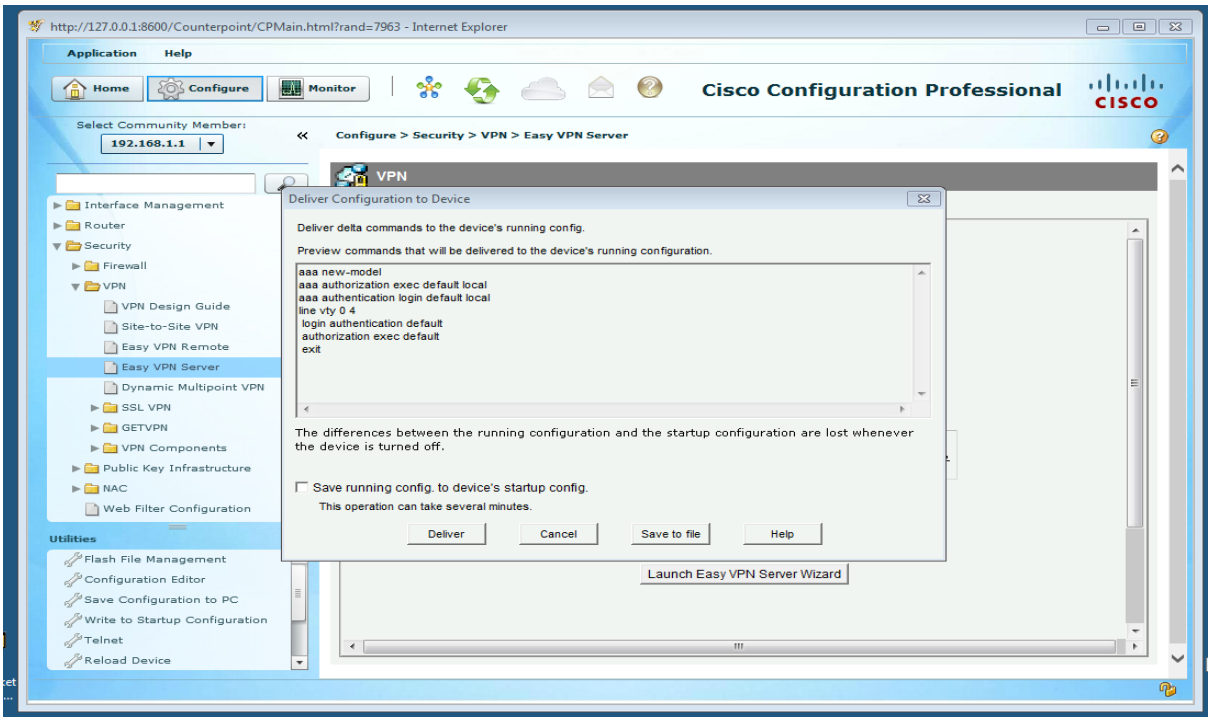
Step 9: Then it goes to the edit fire wall policy screen



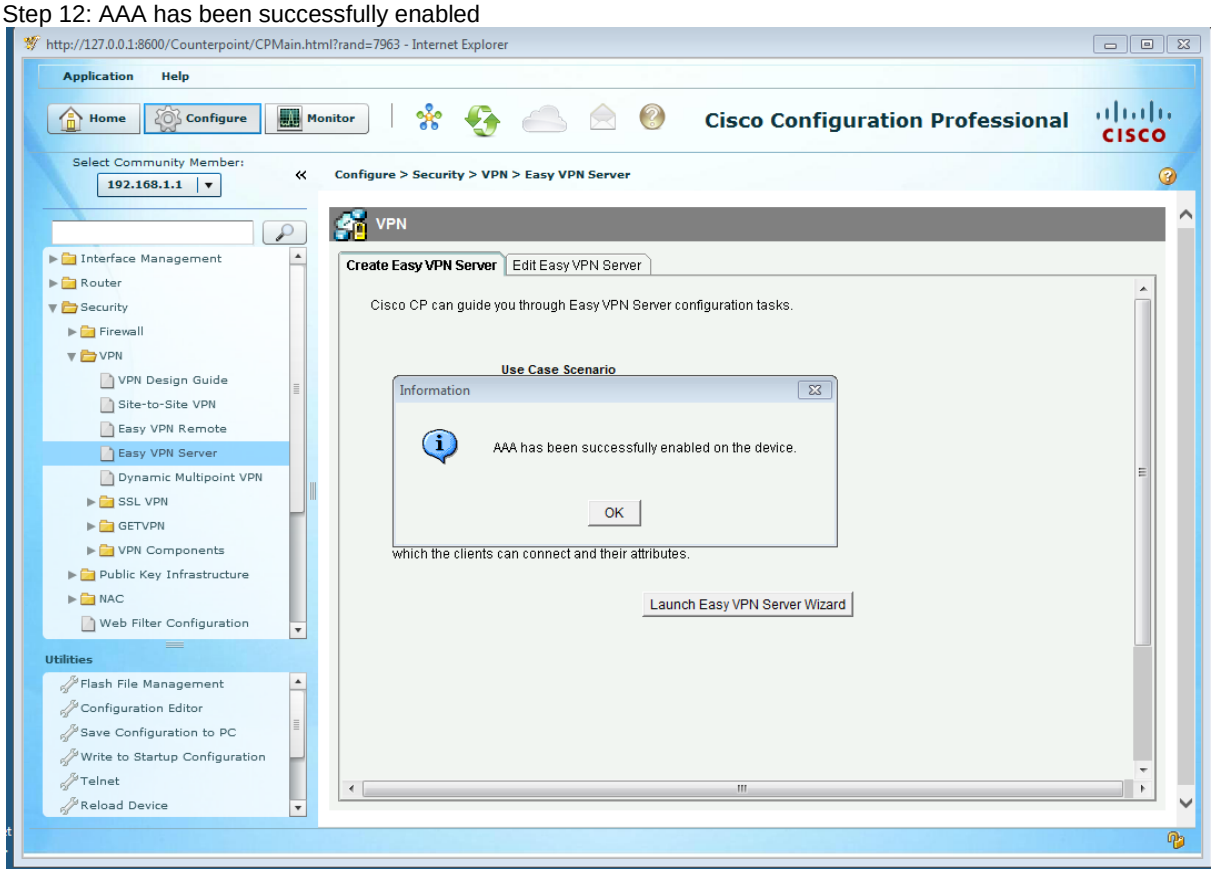
Step 10: Then from CCP AAA needs to be configured



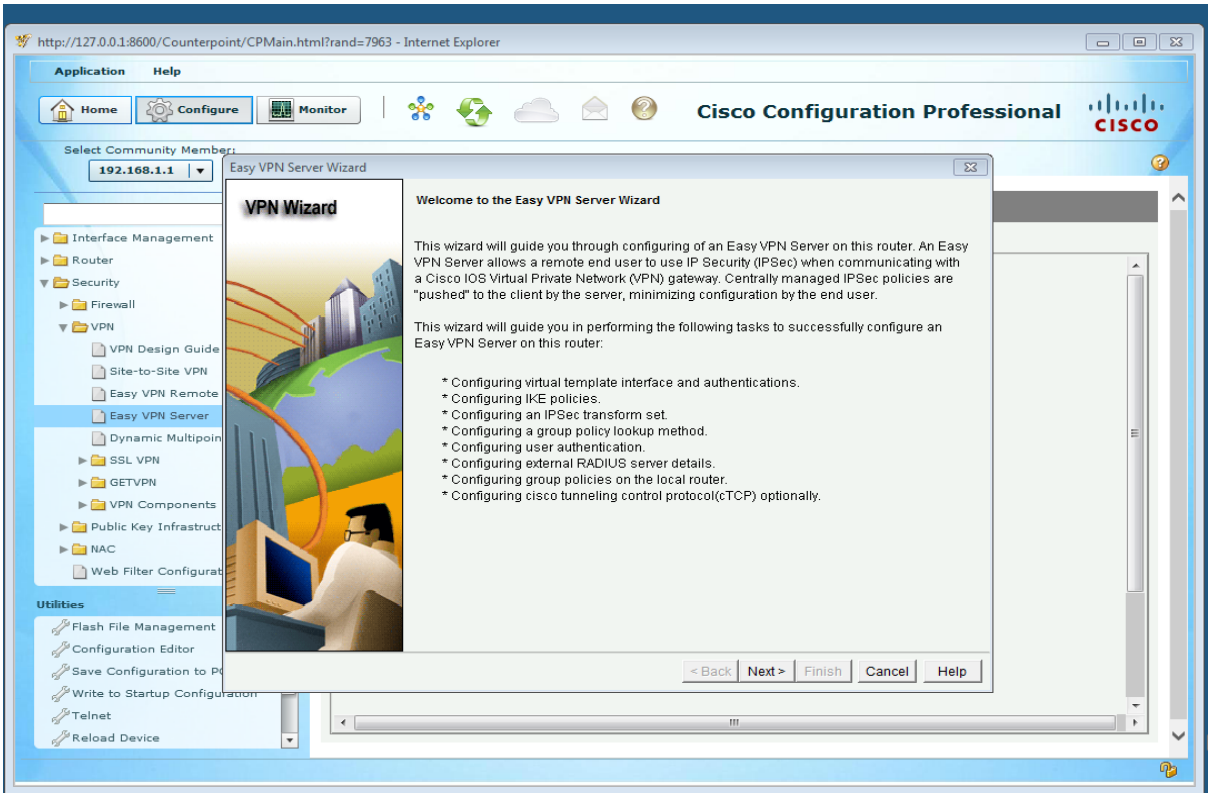
Step 11: The AAA needs to be enabled



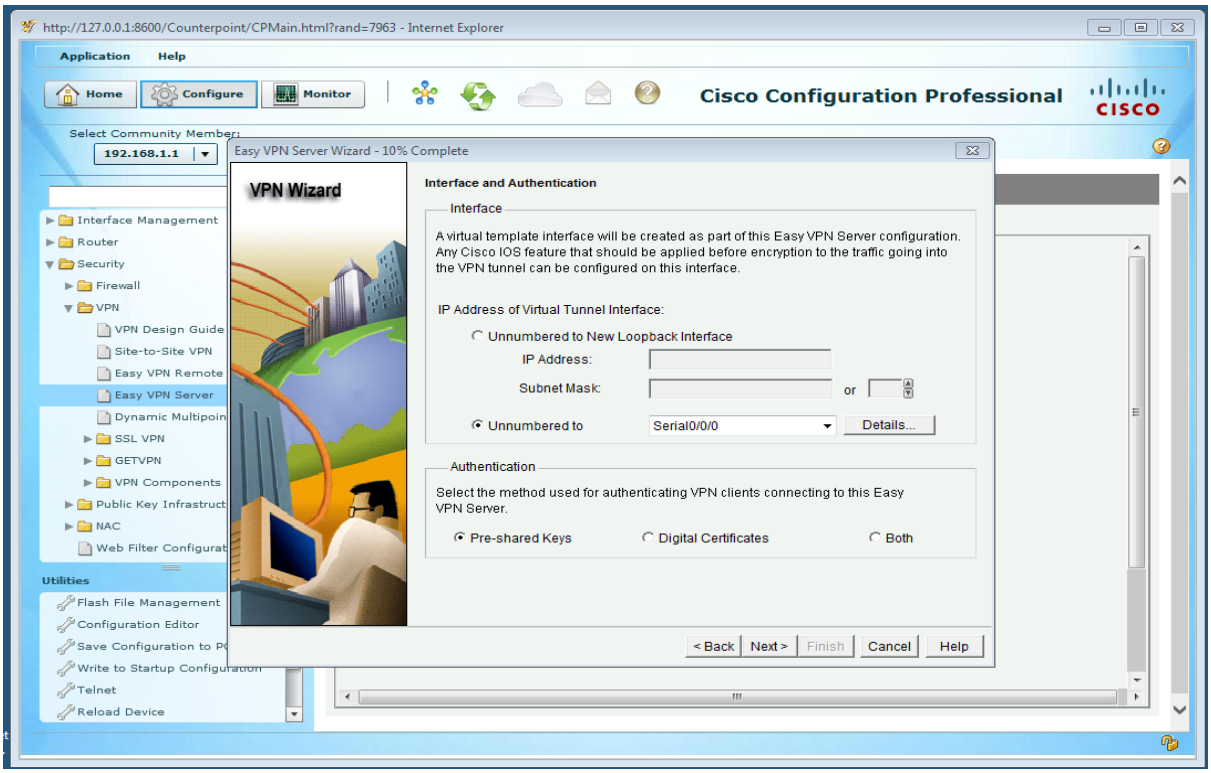
Step 12: AAA has been successfully enabled



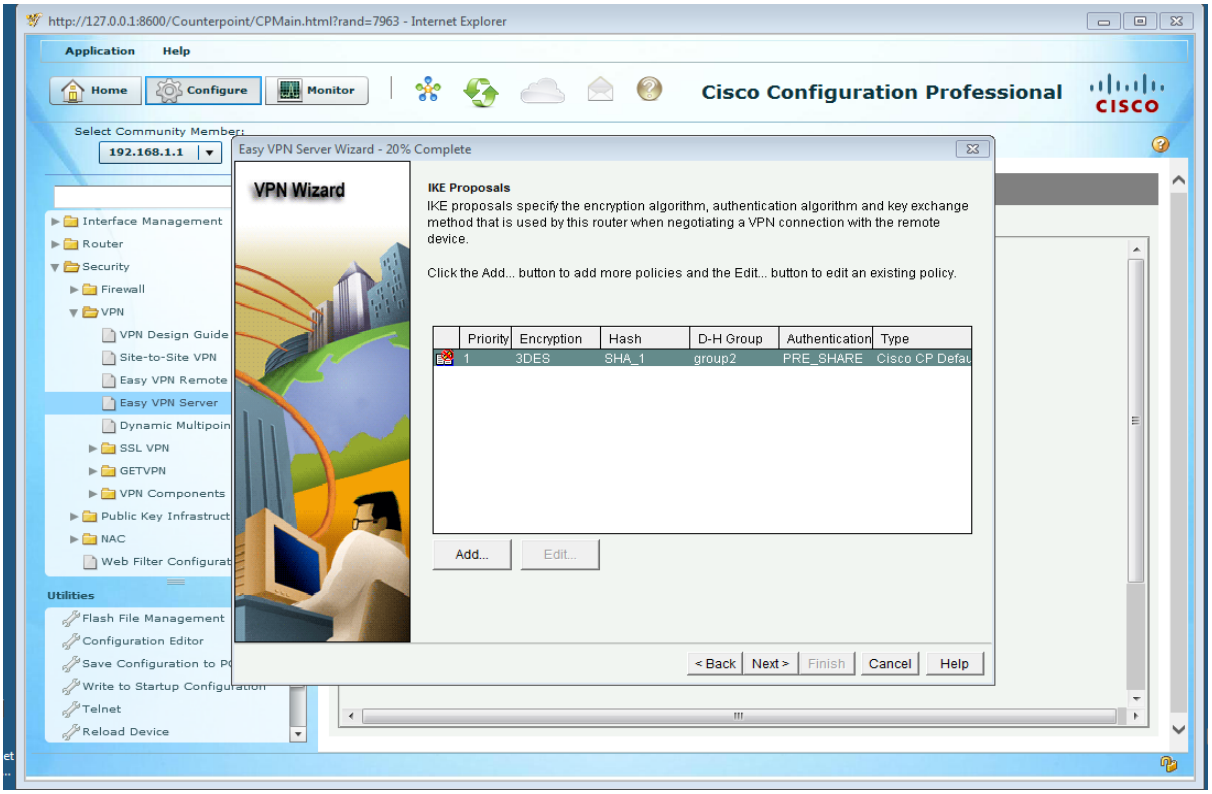
Step 13: Then it comes to the Easy VPN server wizard



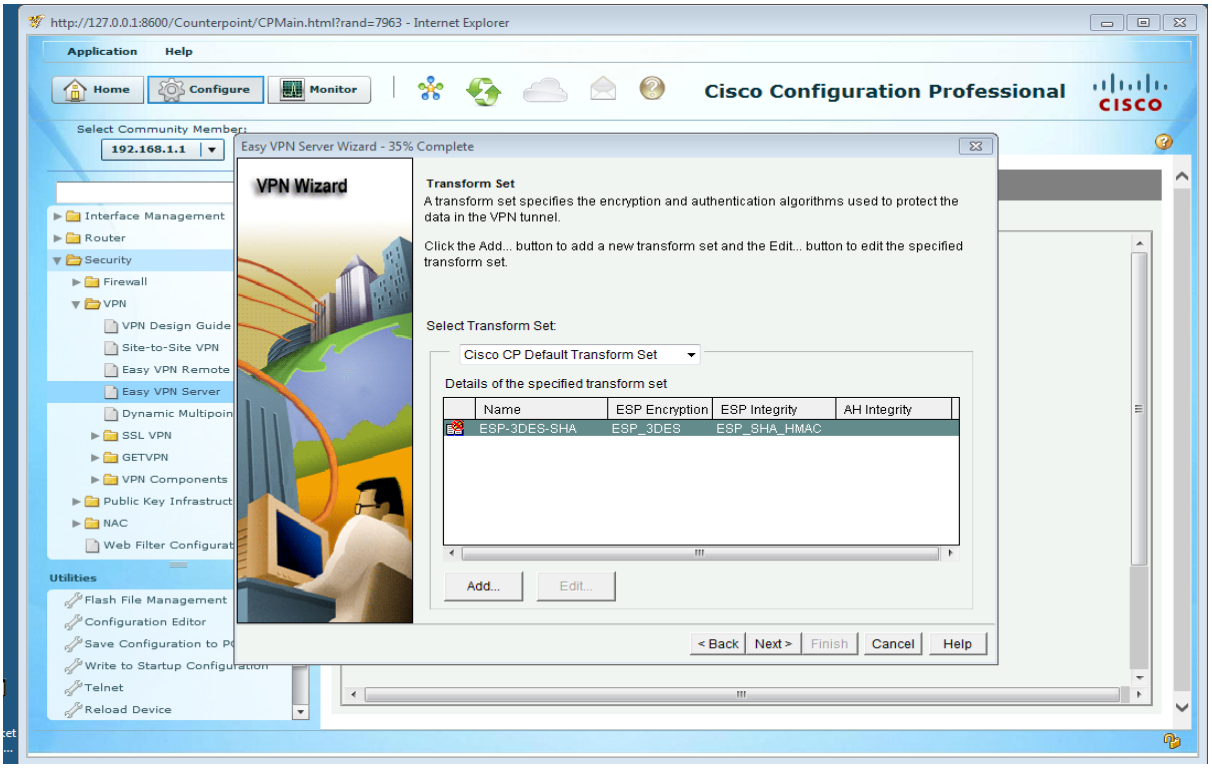
Step 14: Interface and authentication



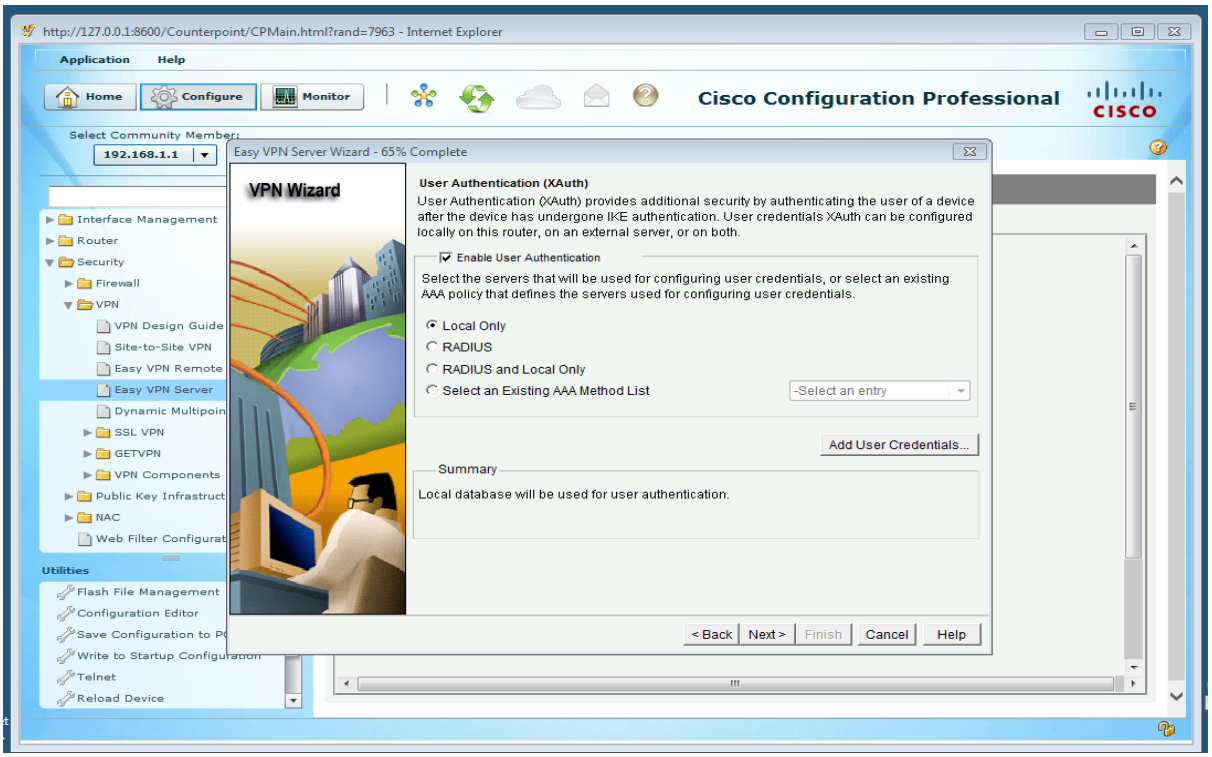
Step 15: The default IKE proposal is used



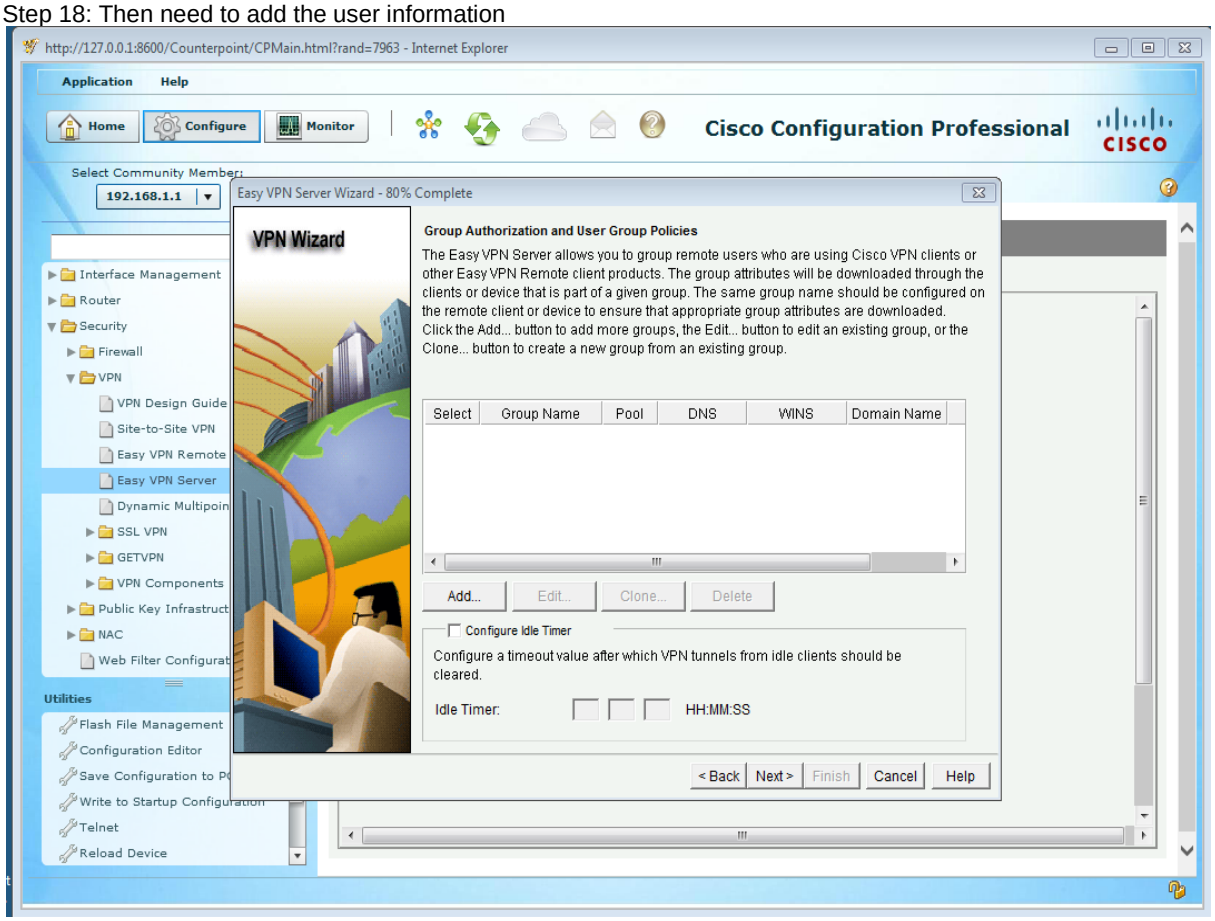
Step 16: The default transform set is used



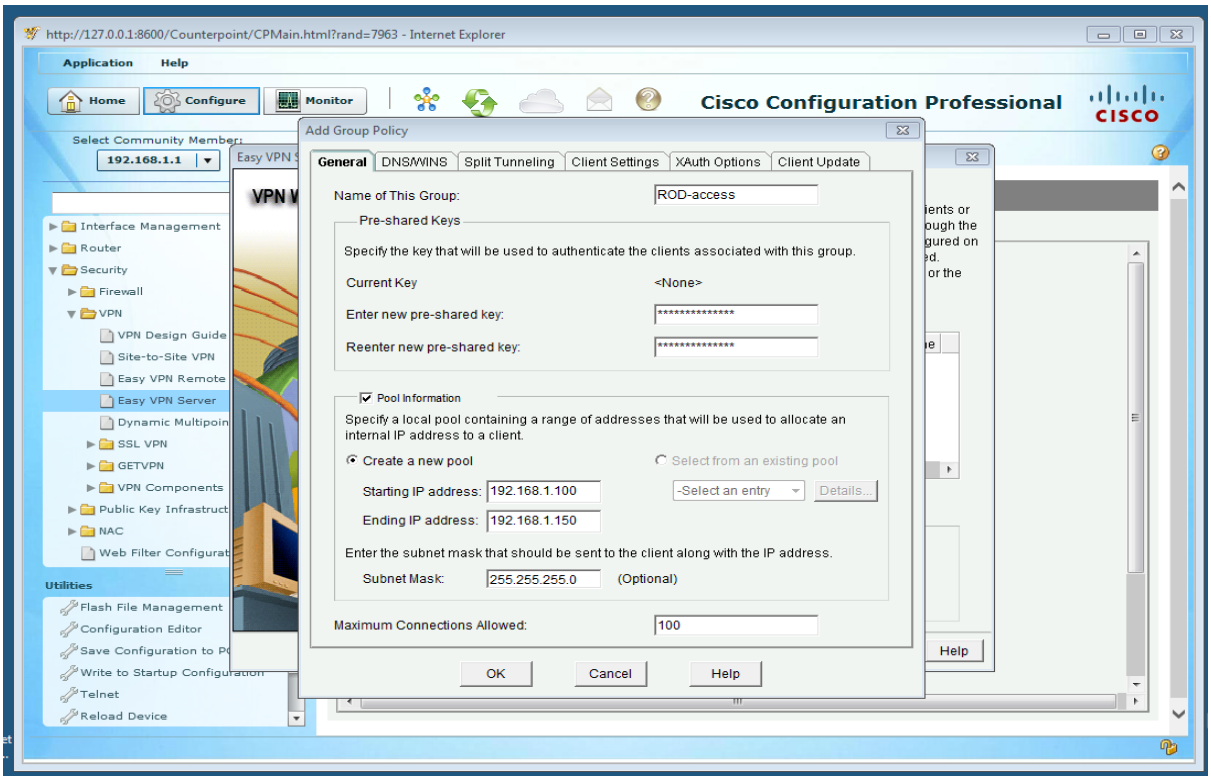
Step 17: In the user authentication local only is being selected



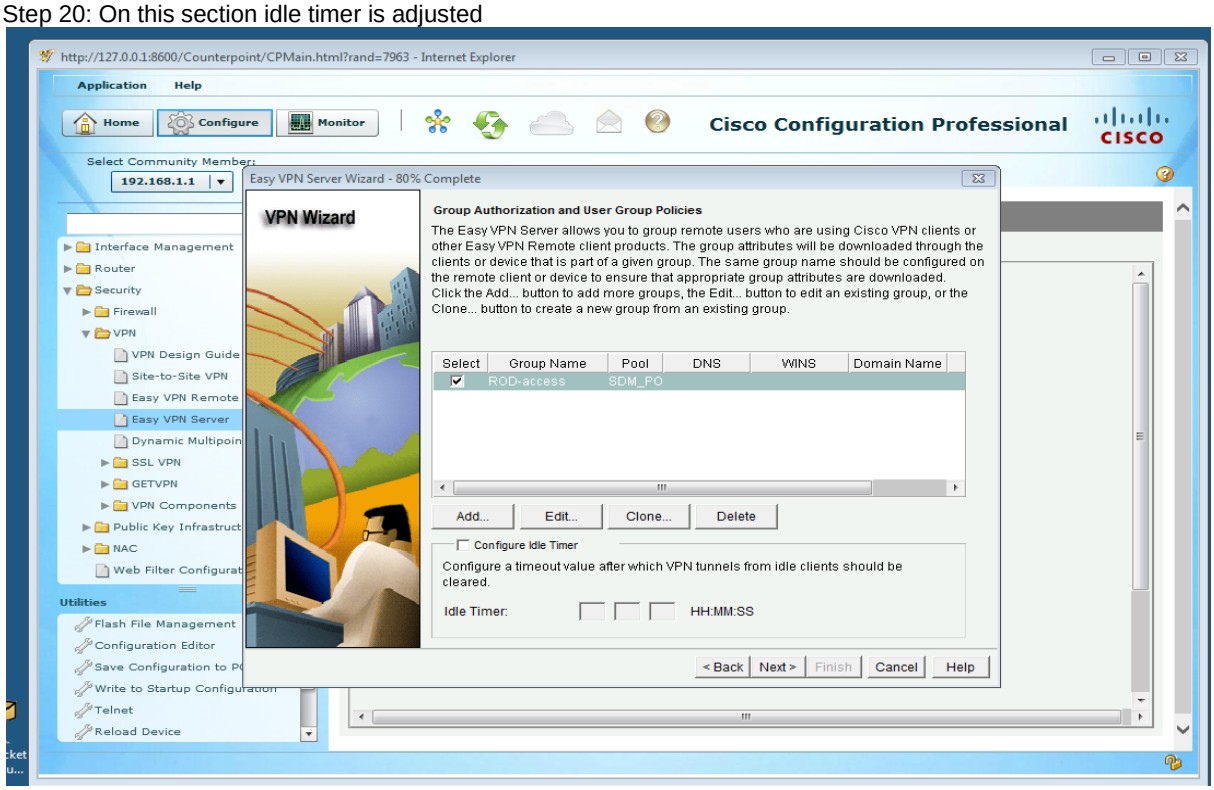
Step 18: Then need to add the user information



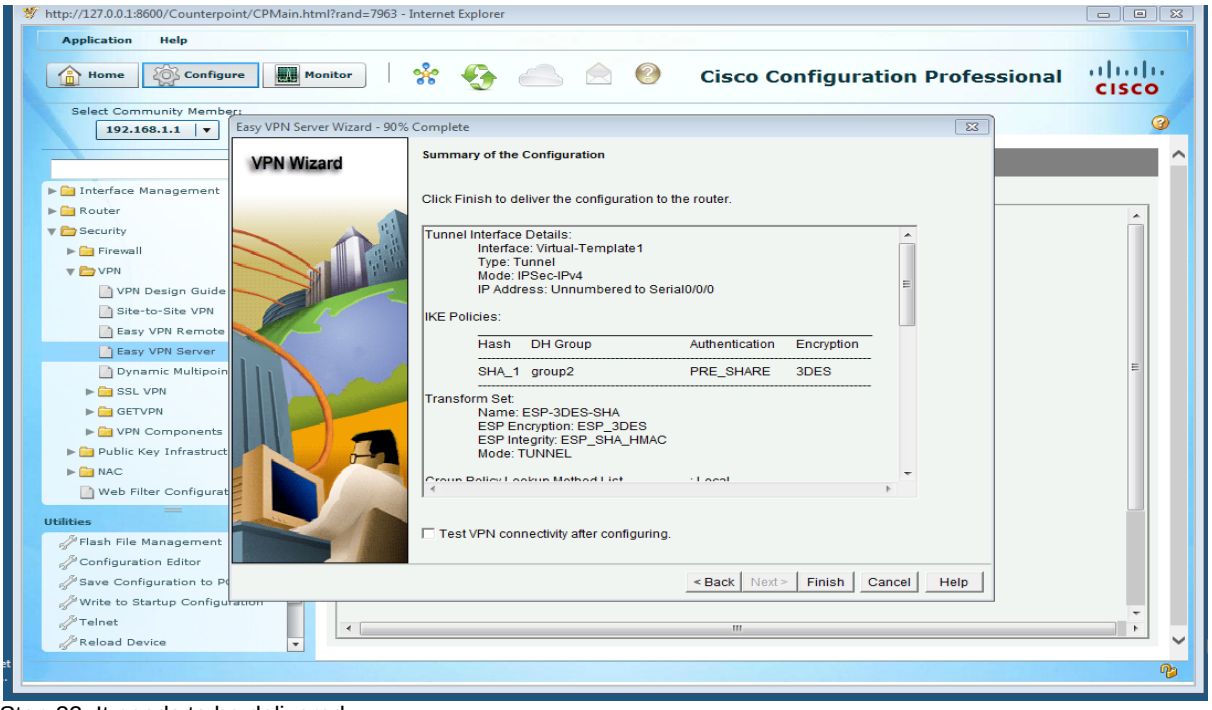
Step 19: Adding a policy for the group, ROD-access



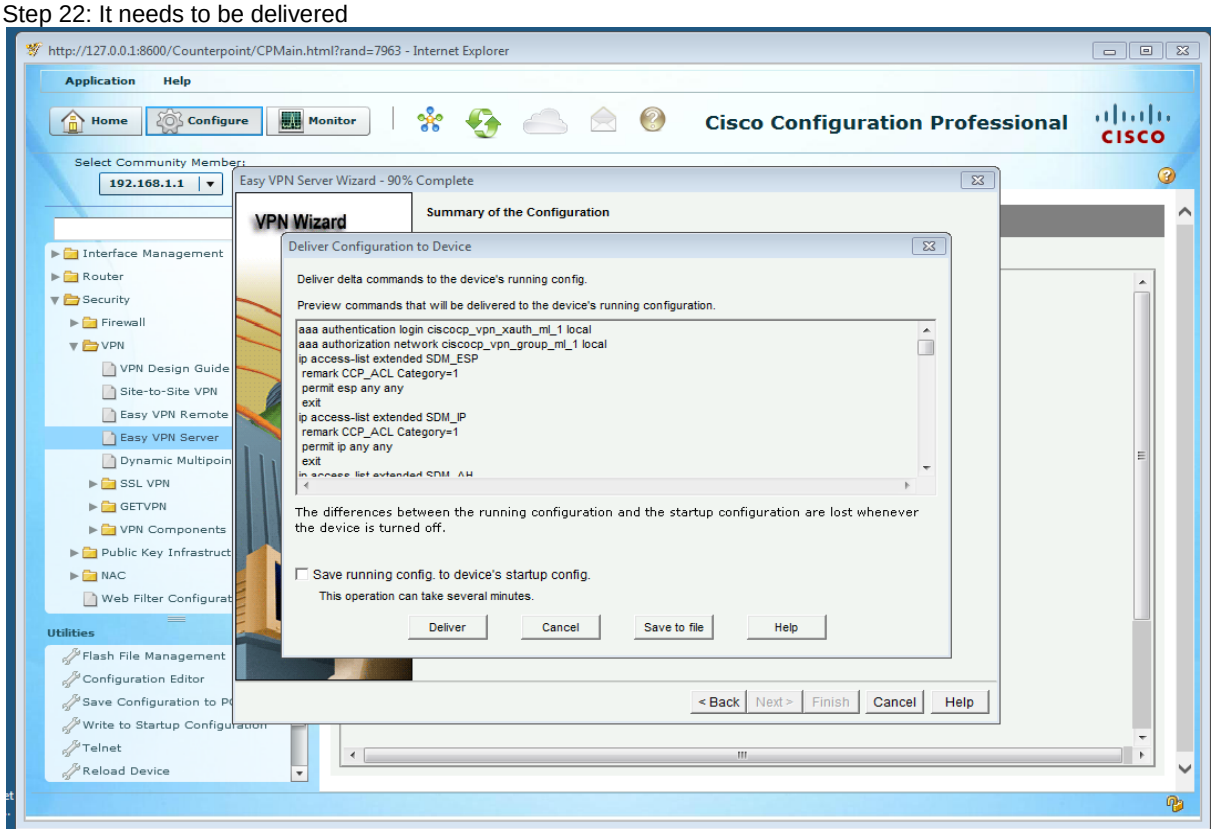
Step 20: On this section idle timer is adjusted



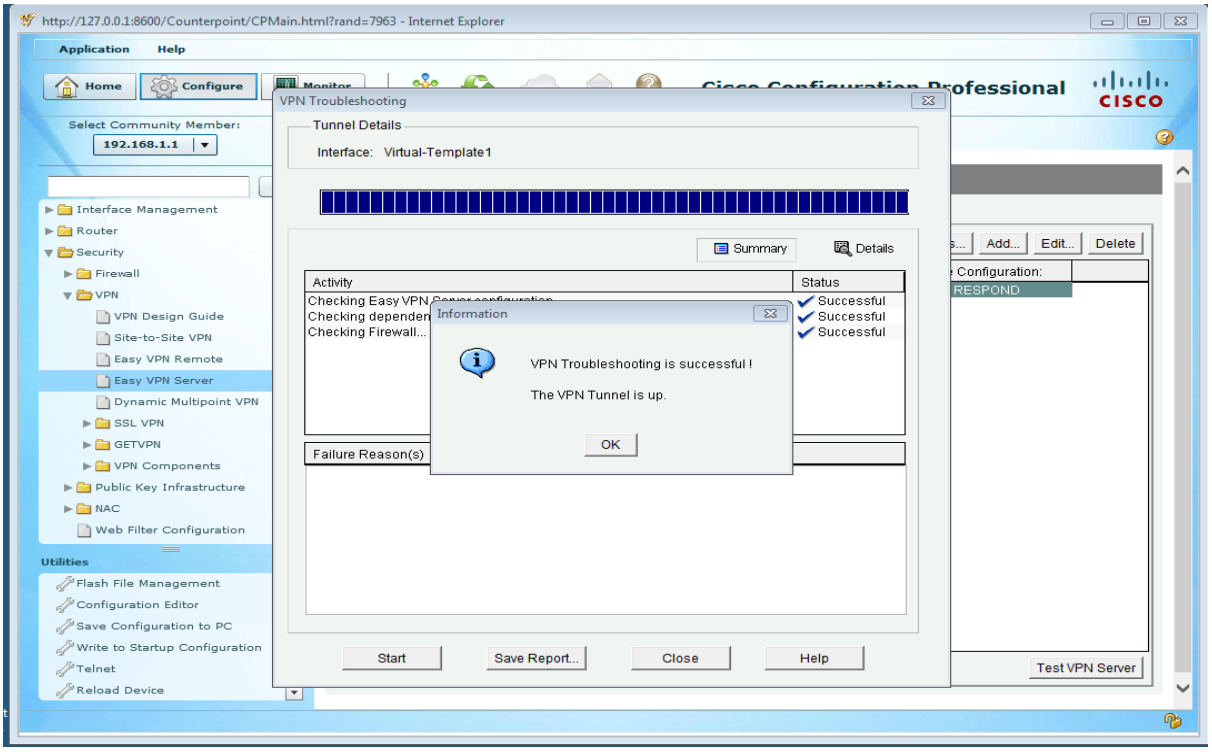
Step 21: shows the final summarization of all the work done



Step 22: It needs to be delivered



Step 23: The tunnel is up.


http://127.0.0.1:8600/Counterpoint/CPMain.html?rand=7963 - Internet Explorer
Application
Help
Home
Configure
Monitor
Cisco Configuration Professional
CISCO
Select Community Member:
192.168.1.1
Interface Management
Router
Security
Firewall
VPN
VPN Design Guide
Site-to-Site VPN
Easy VPN Remote
Easy VPN Server
Dynamic Multipoint VPN
SSL VPN
GETVPN
VPN Components
Public Key Infrastructure
NAC
Web Filter Configuration
Utilities
Flash File Management
Configuration Editor
Save Configuration to PC
Write to Startup Configuration
Telnet
Reload Device
VPN Troubleshooting
Tunnel Details
Interface: Virtual-Template1
Summary
Details
Activity
Status
Checking Easy VPN
Checking dependen
Checking Firewall...
Successful
Successful
Successful
Information
VPN Troubleshooting is successful !
The VPN Tunnel is up.
OK
Failure Reason(s)
Start
Save Report...
Close
Help
Add...
Edit...
Delete
Configuration:
RESPOND
Test VPN Server

Appendix 7: Secure Sockets Layer configuration on R1

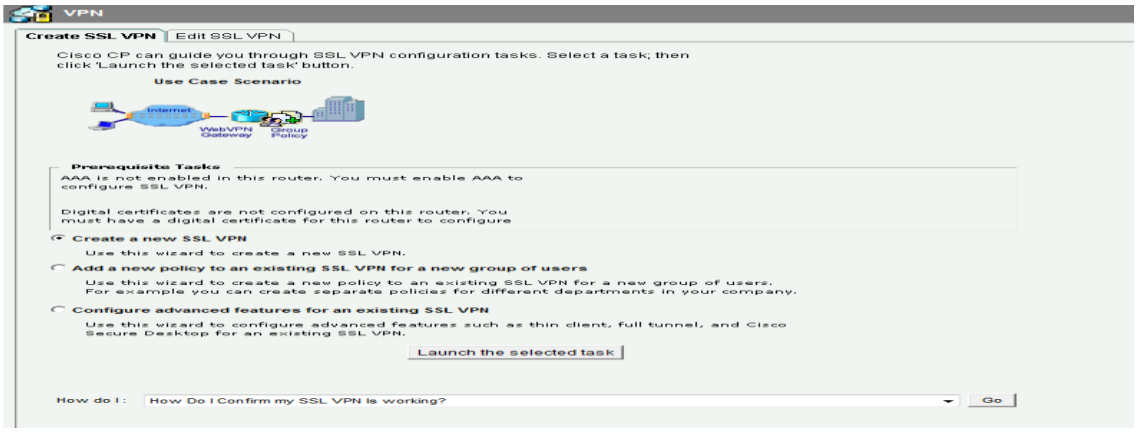
```
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable password 7 104F0D140C190004080D7B7977
!
aaa new-model
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
!
aaa session-id common
!
memory-size iomem 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint test_trustpoint_config_created_for_sdm
 subject-name e=sdmtest@sdmtest.com
 revocation-check crl
!
crypto pki trustpoint R1_Certificate
 enrollment selfsigned
 serial-number none
 ip-address none
 revocation-check crl
 rsakeypair R1_Certificate_RSAKey 512
!
crypto pki certificate chain test_trustpoint_config_created_for_sdm
crypto pki certificate chain R1_Certificate
 certificate self-signed 01
  3082016A 30820114 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  13311130 0F06092A 864886F7 0D010902 16025231 301E170D 31353034 32303130
  32303435 5A170D32 30303130 31303030 3030305A 30133111 300F0609 2A864886
  F70D0109 02160252 31305C30 0D06092A 864886F7 0D010101 0500034B 00304802
  41009CEB 6E9321FC 34C658BF 45B7E029 7B65CB91 370D6B76 9DEE4243 B892322E
  C27ACE49 8C8723AC 9B542930 1CBA590D 87ED024B 212F472C 38510718 981C3D39
  0C5F0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14BDCB2B 823CE7CB F1624DF9 D7A8E43C 03CA10F1 21301D06
  03551D0E 04160414 BDCB2B82 3CE7CBF1 624DF9D7 A8E43C03 CA10F121 300D0609
  2A864886 F70D0101 05050003 41005C9A D9C4482F C06329E9 A720C23D 4C7E3FF3
  2790460F 0F21B95A B8632F87 08B8F211 6577CE9A 82150954 AA3A0EC2 B24E2A74
  6403555D 4833CB87 0D275DD2 10FE
        quit
!
license udi pid CISCO2811 sn FCZ133770S6
vtp domain TSHOOT
vtp mode transparent
```

```
username adminrodi privilege 15 password 7 045A0F0B062F5E410D10544541
!
redundancy
!
ip ssh version 1
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Virtual-Template1
 ip unnumbered Serial0/0/0
!
router eigrp 101
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
!
ip forward-protocol nd
ip http server
no ip http secure-server
!
ip flow-export version 9
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
no cdp run
!
control-plane
!
mgcp profile default
!
line con 0
 exec-timeout 0 0
 password 7 094F471A1A0A141D051C053938
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 0 0
 password 7 104D000A0618041F15142B3837
 transport input all
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
 ip address 10.1.1.1 port 443
 http-redirect port 80
 ssl trustpoint R1_Certificate
 inservice
```

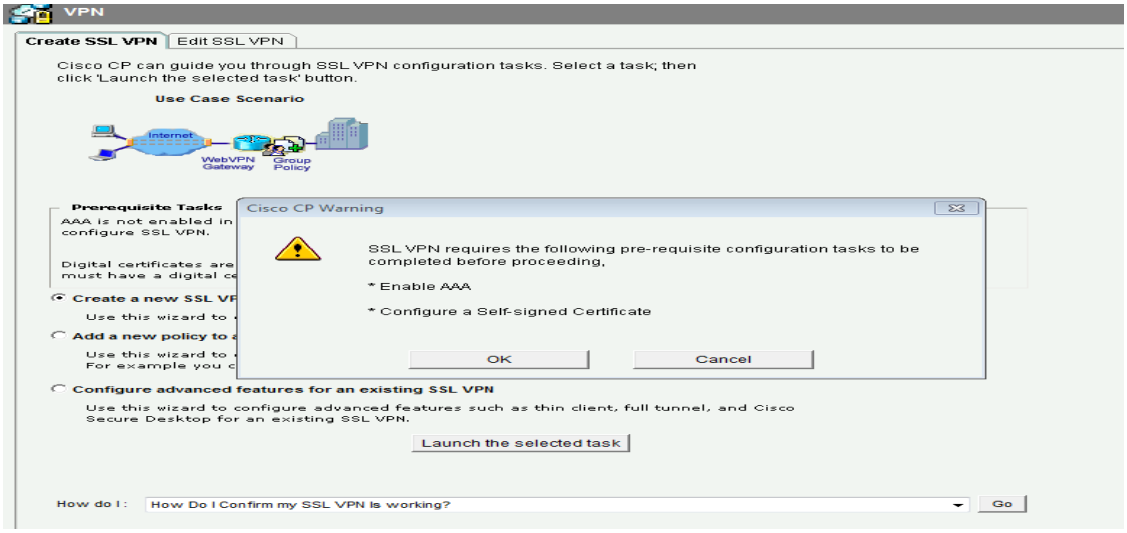
```
 !
webvpn context adminrodi
 secondary-color white
 title-color #CCCC66
 text-color black
 ssl authenticate verify all
 !
 policy group policy_1
 virtual-template 1
 default-group-policy policy_1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 max-users 50
 inservice
!
end
```

Appendix 8.Secure Sockets Layer Configuration using VPN Wizard on R1

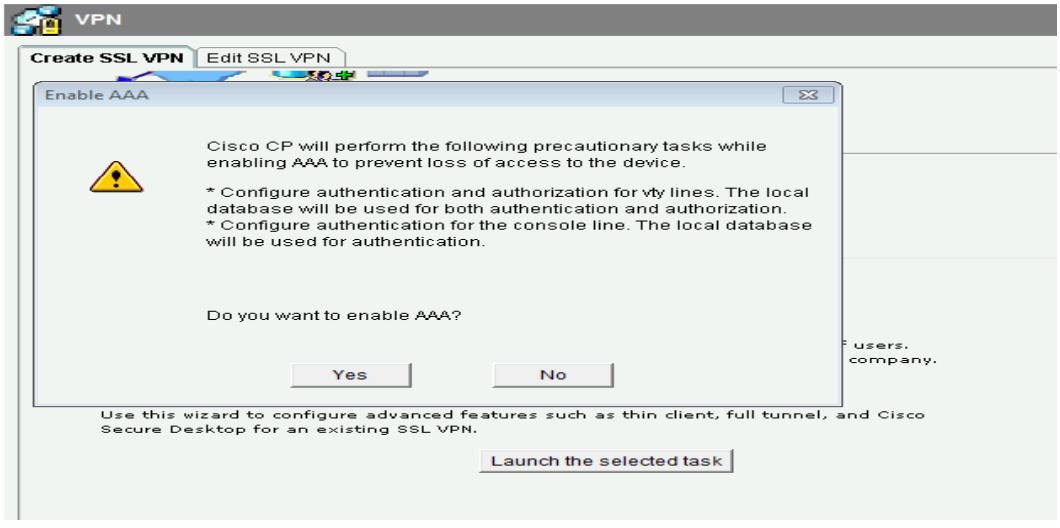
Step 1: The SSL VPN manager



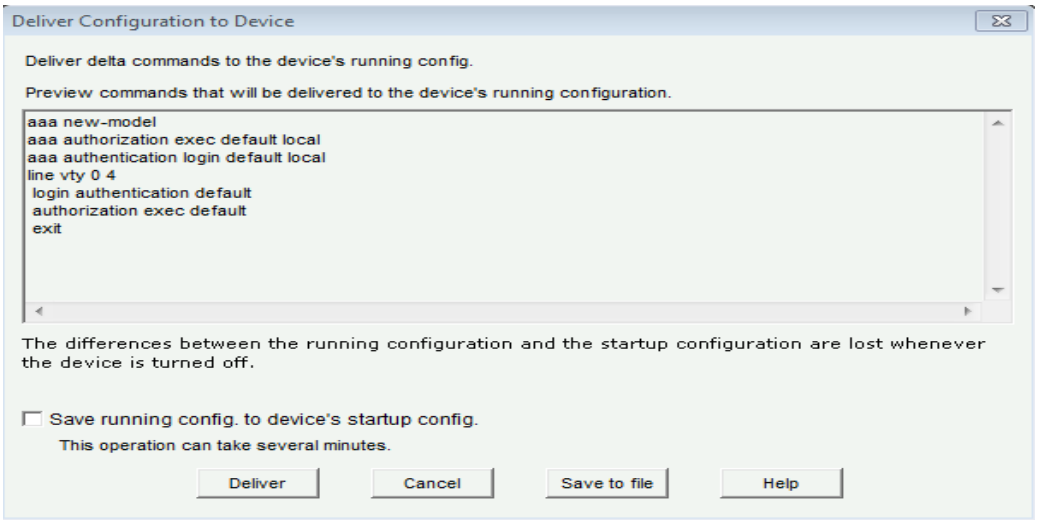
Step 2: Enabling AAA and configuring a self signed certificate



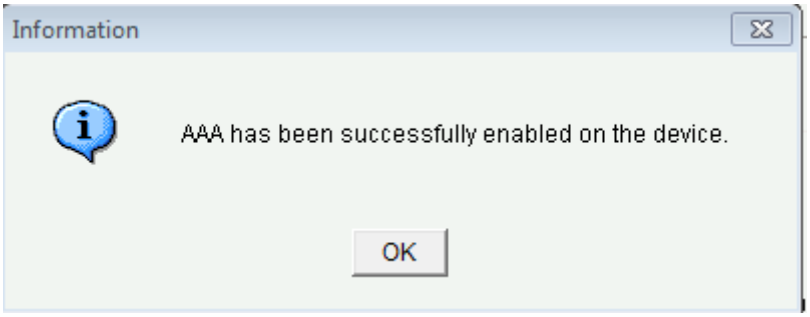
Step 3: Enabling AAA



Step 4: Delivering configuration to device

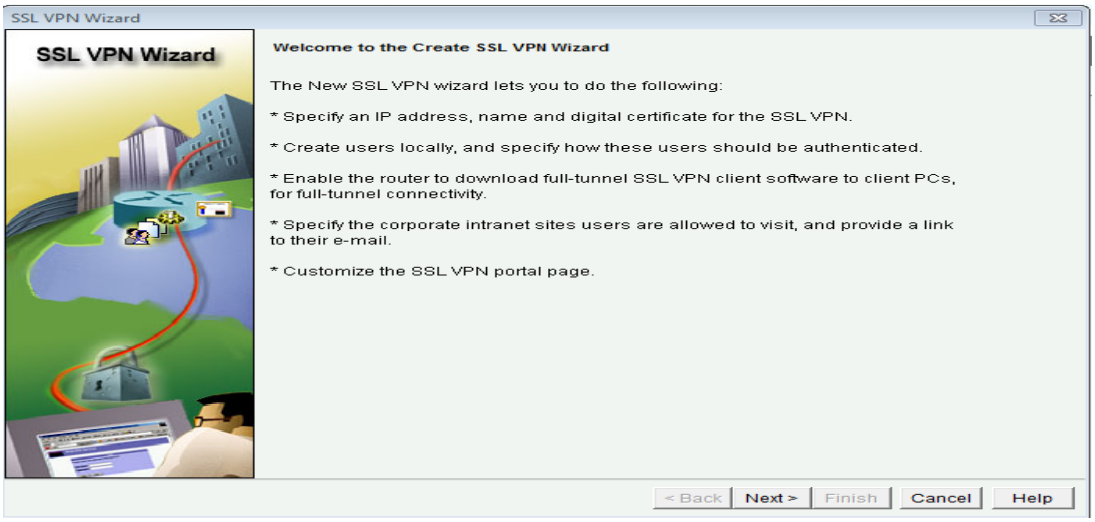


Step 5: Enabling AAA completed

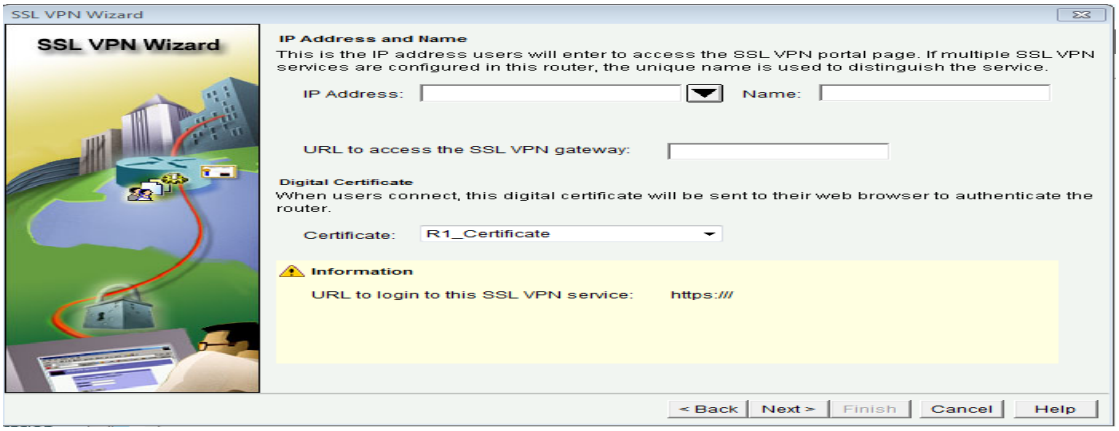


Step 6: self signed certificated created successfully

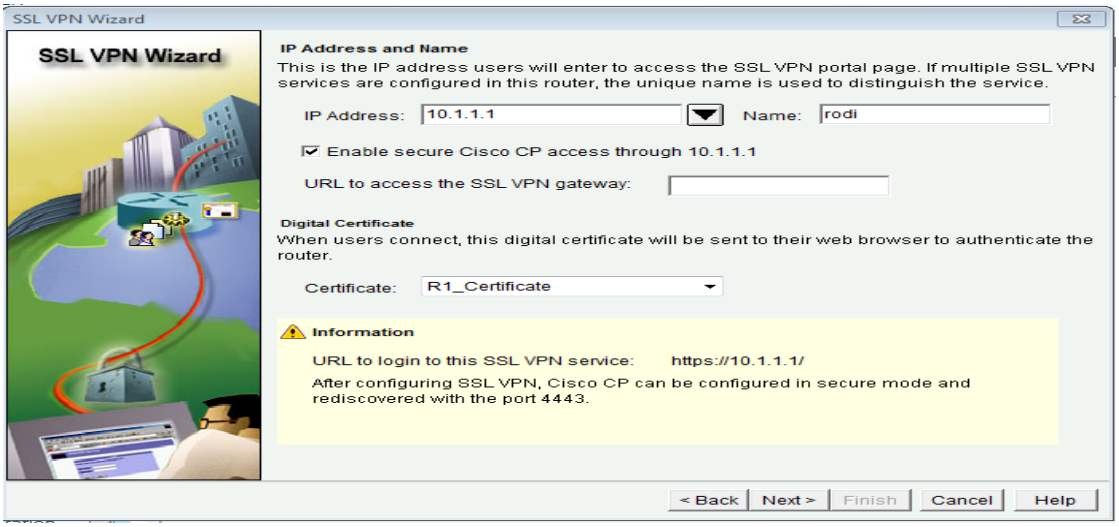
Step 7: The SSL VPN Wizard



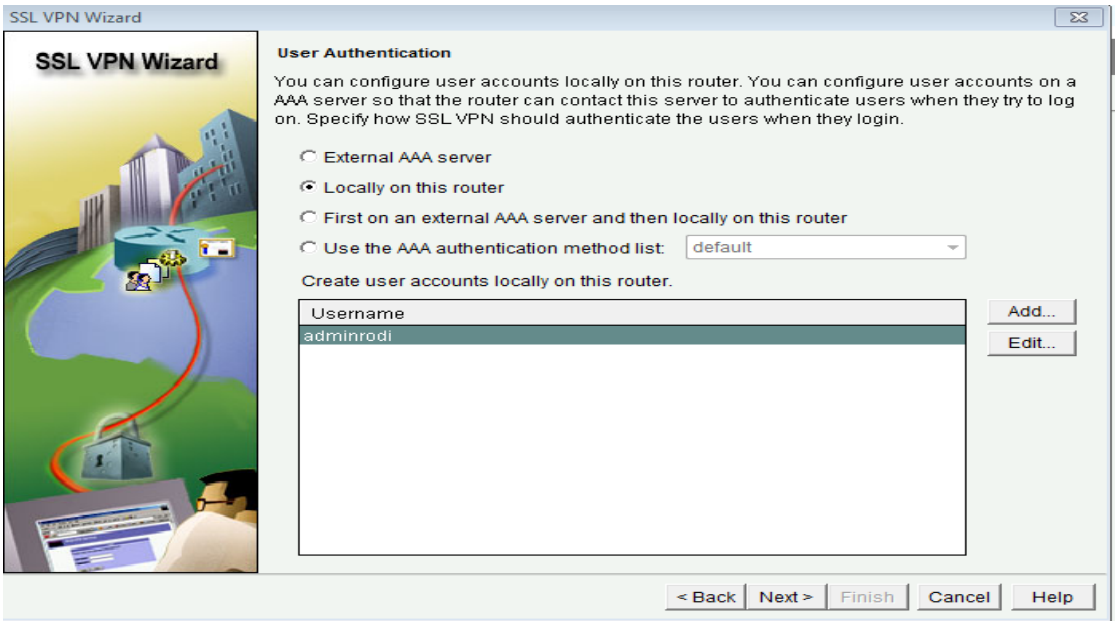
Step 8: SSL VPN ip address and name for SSL VPN



Step 9: Entering SSL VPN ip address and name for SSL VPN

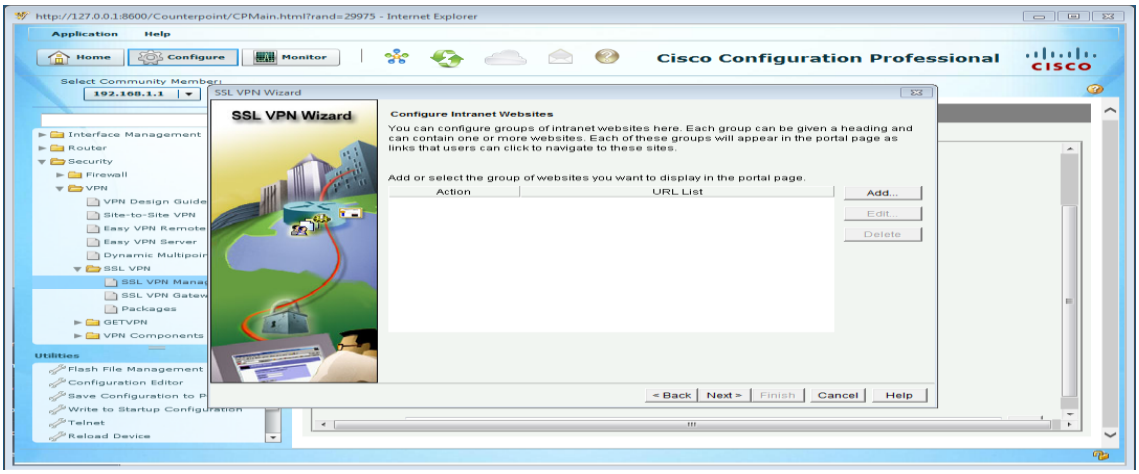


Step 10: Adding users of the VPN

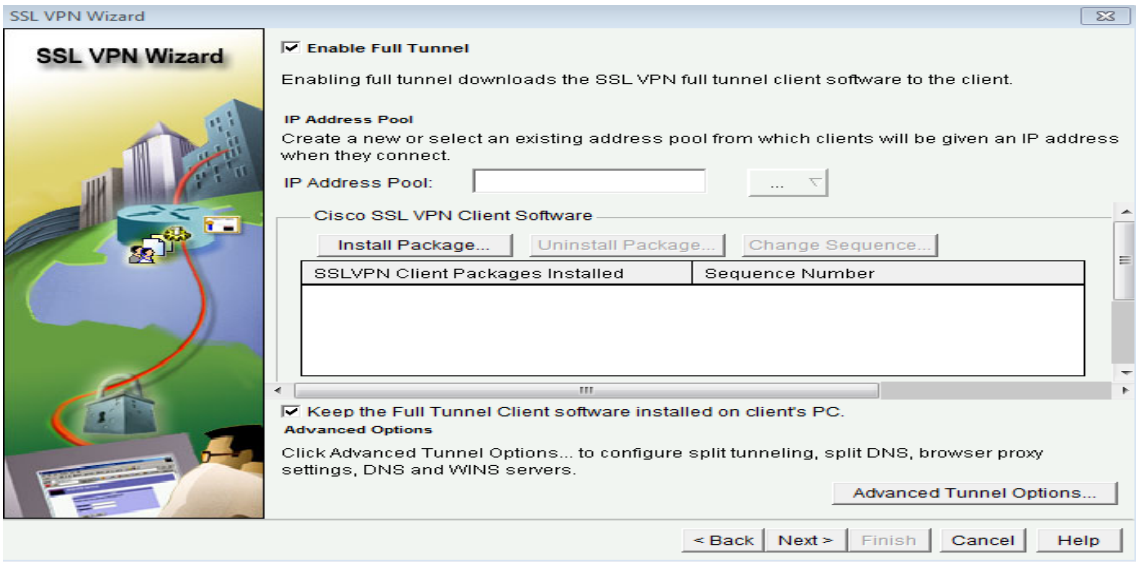


Step 11: Adding an account for the VPN user

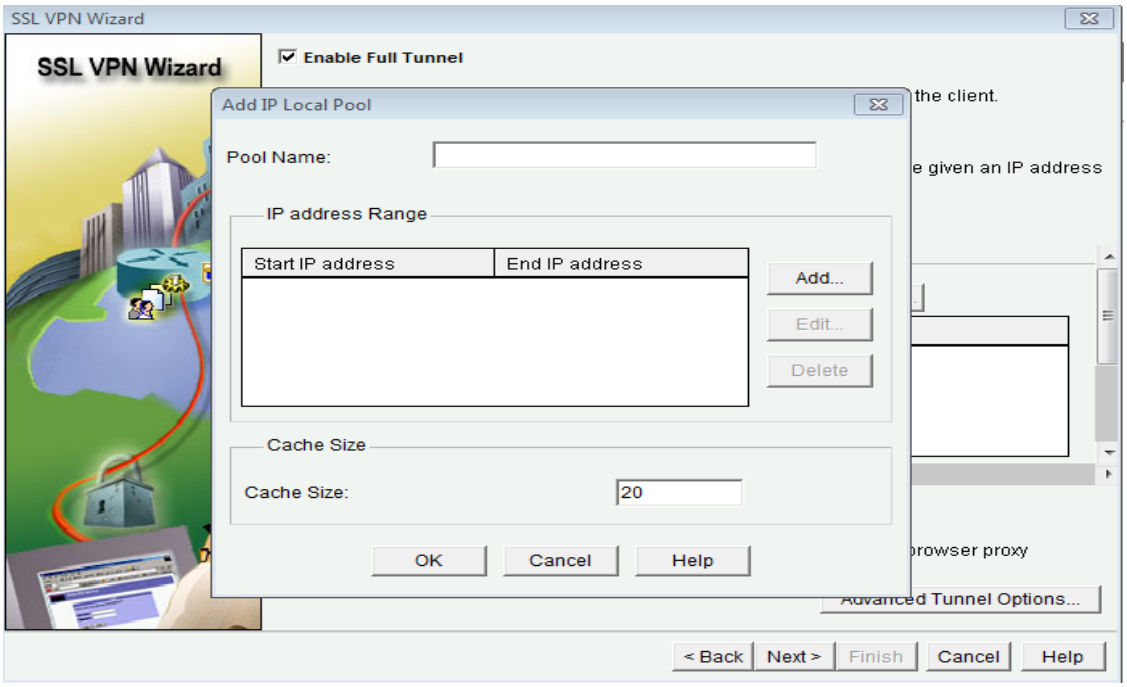
Step 12: Configuring the intranet websites



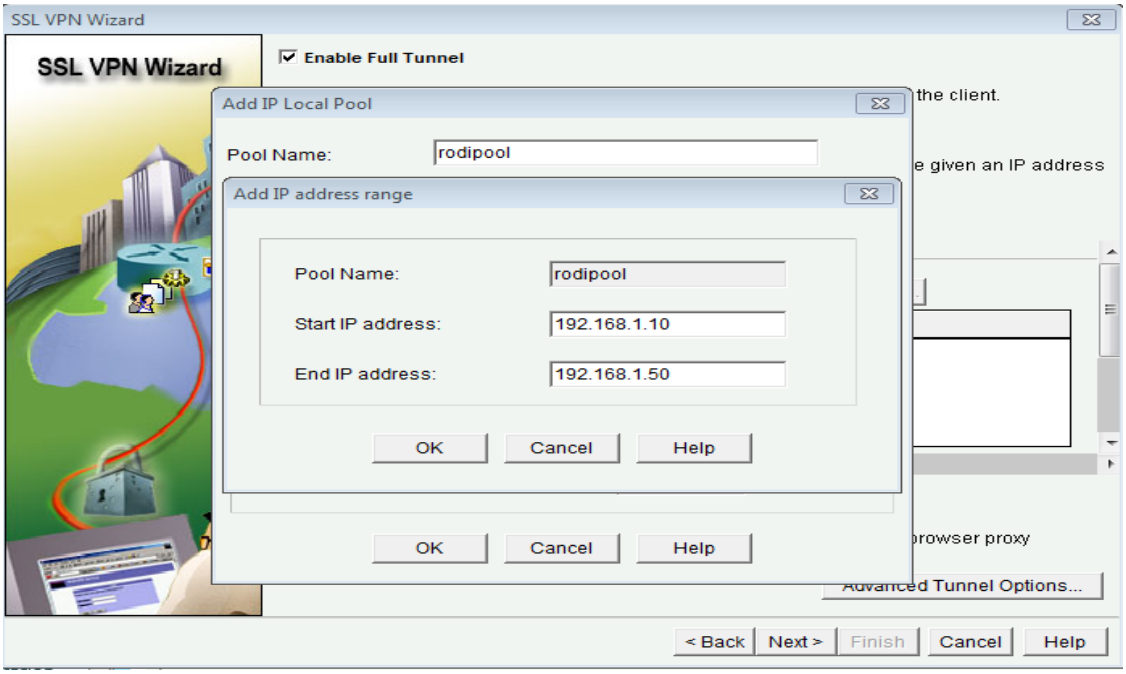
Step 13: Adding Ip address pool



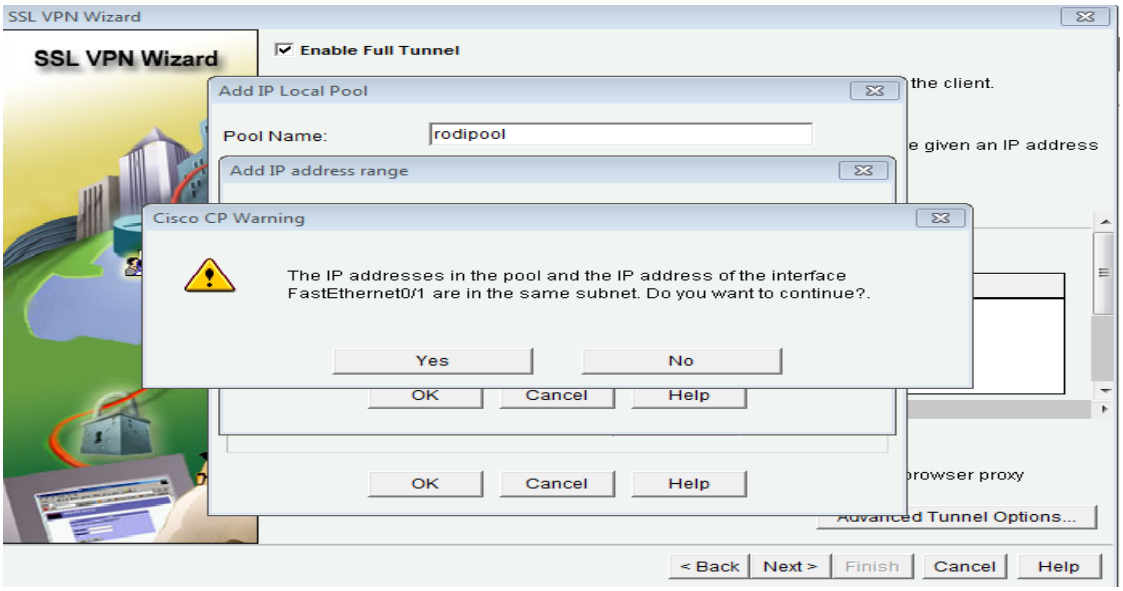
Step 14: Adding IP local pool



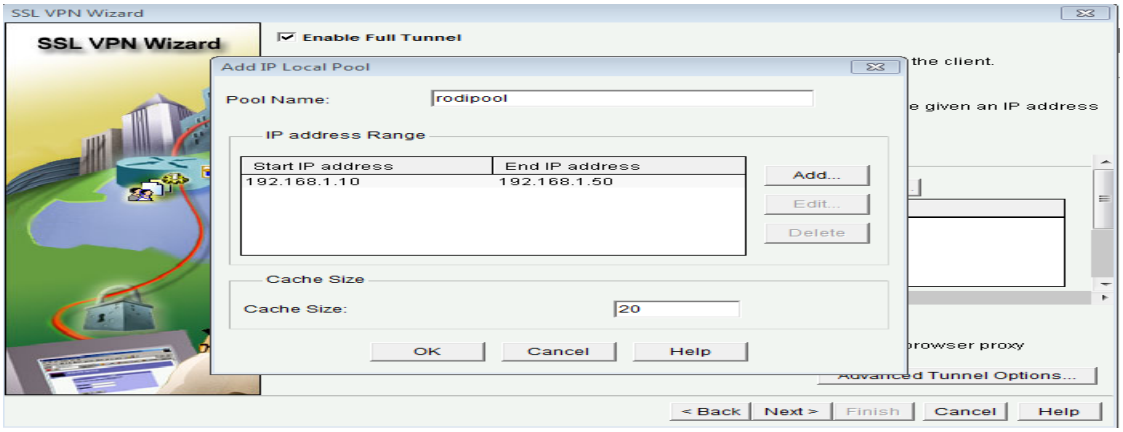
Step 15: Adding IP address range



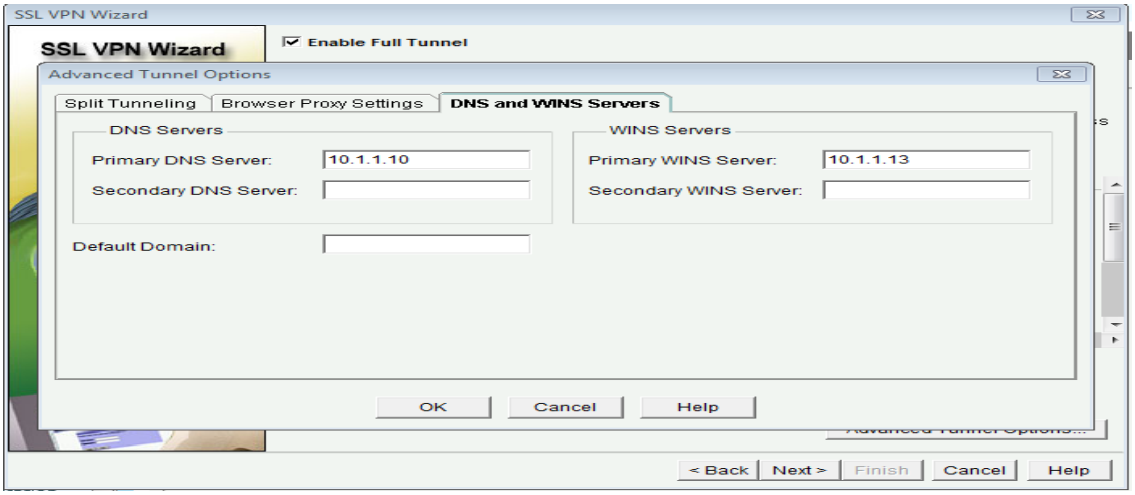
Step 16: confirming the IP address range



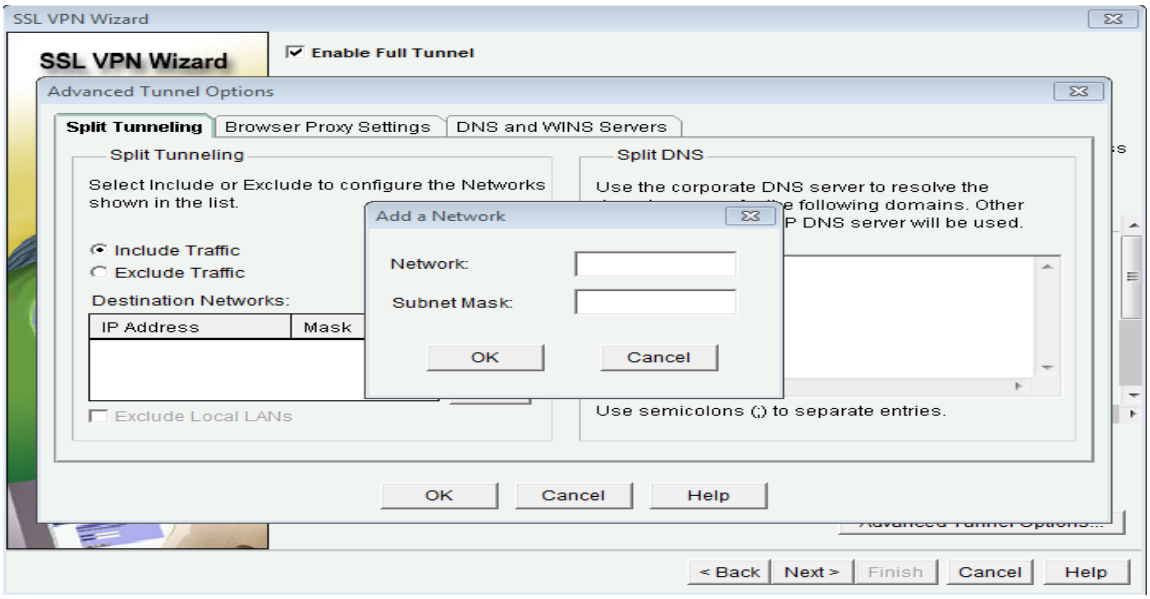
Step 17: The IP local pool is added



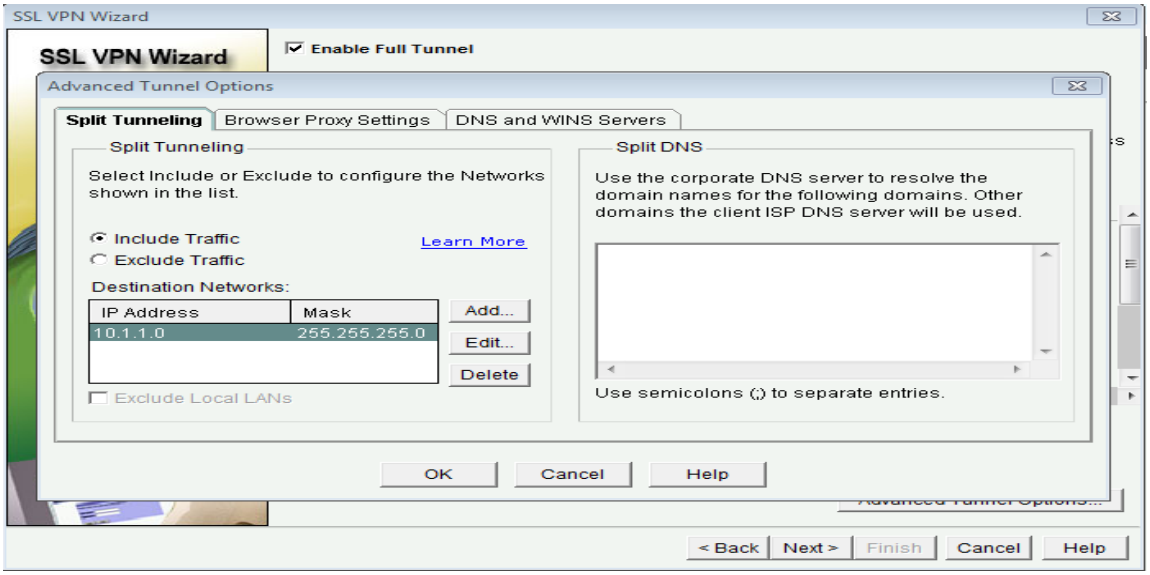
Step 18: Adding DNS server and WINS server



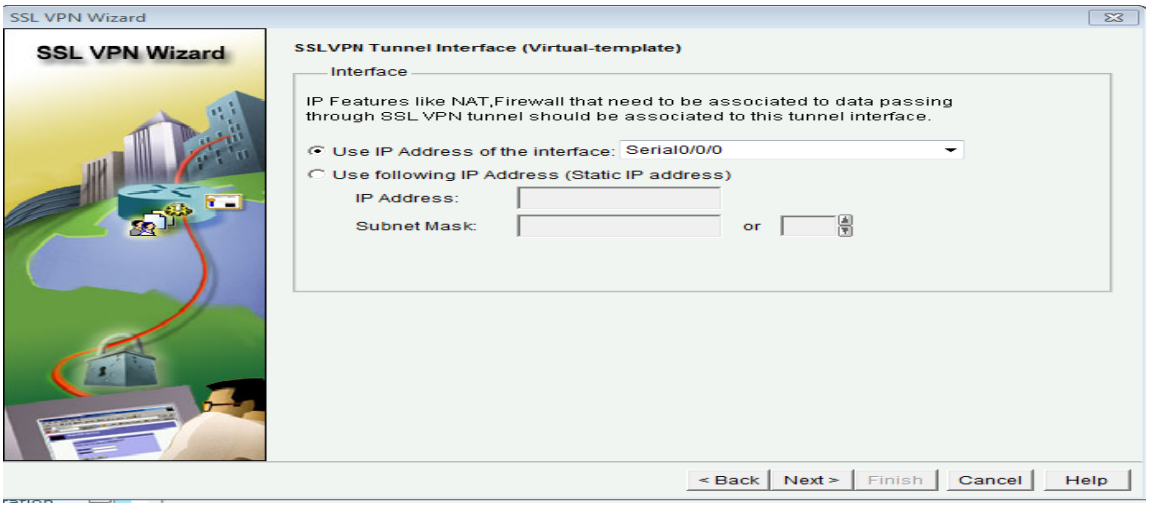
Step 19: Split Tunneling



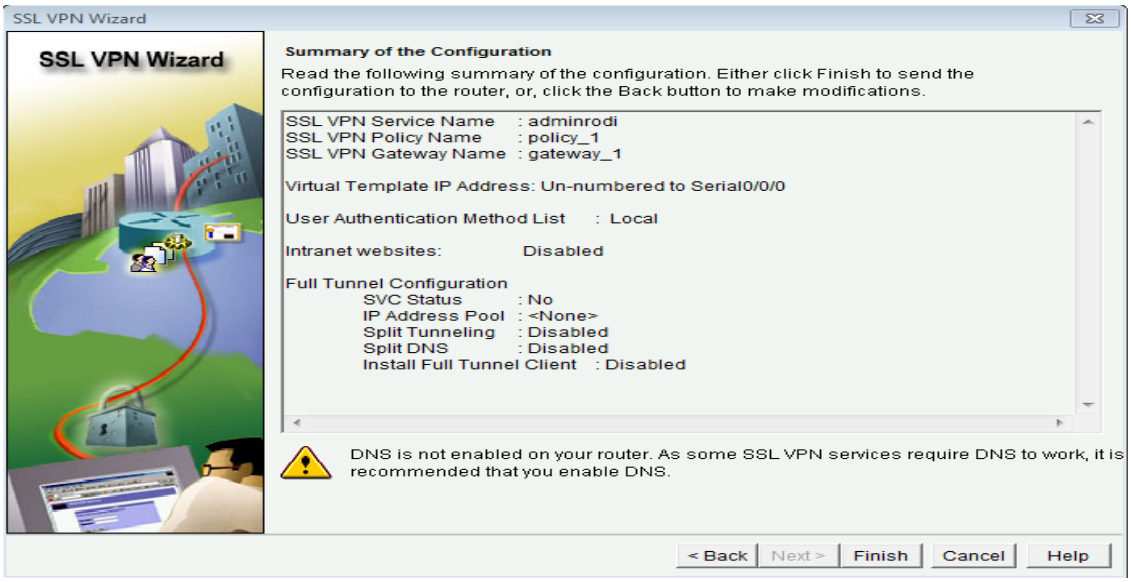
Step 20: Split Tunneling added



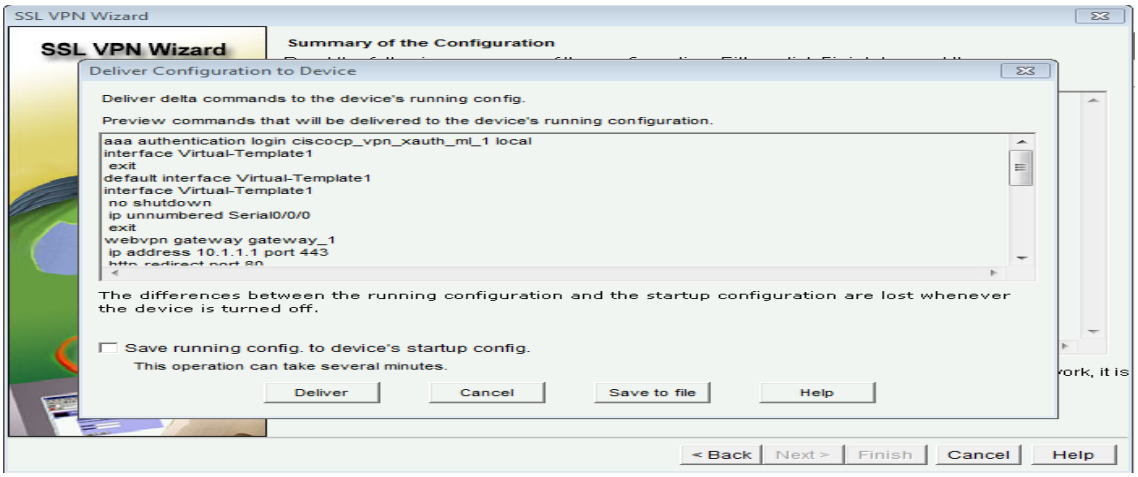
Step 21: Adding VPN Tunnel Interface



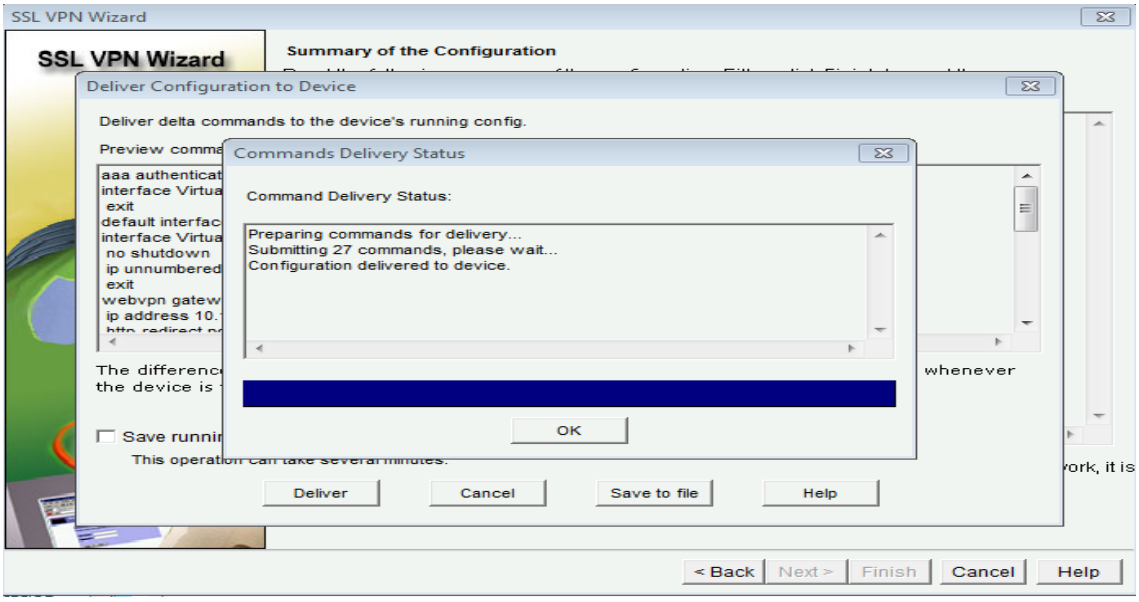
Step 22: Summery of the overall configuration



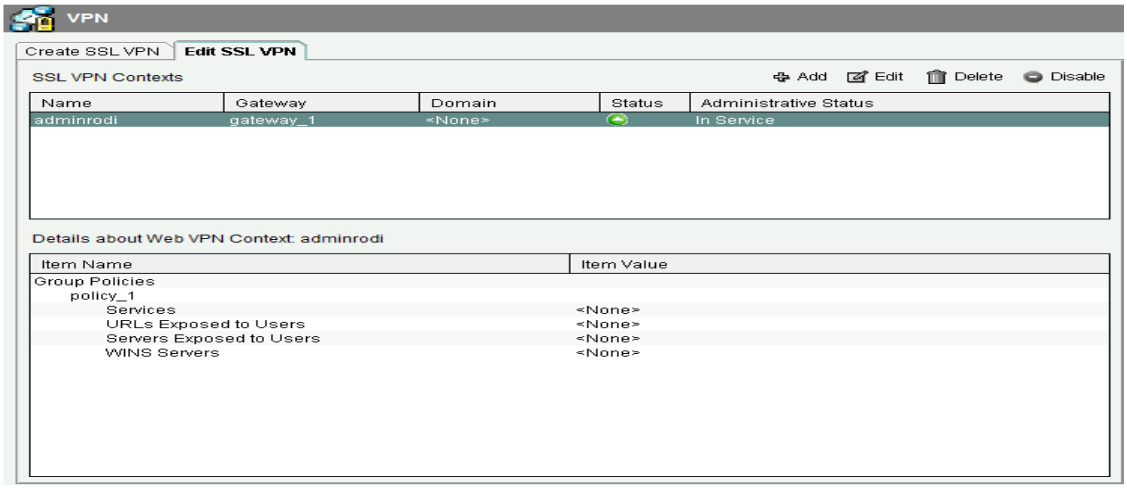
Step 23: Delivering the summary



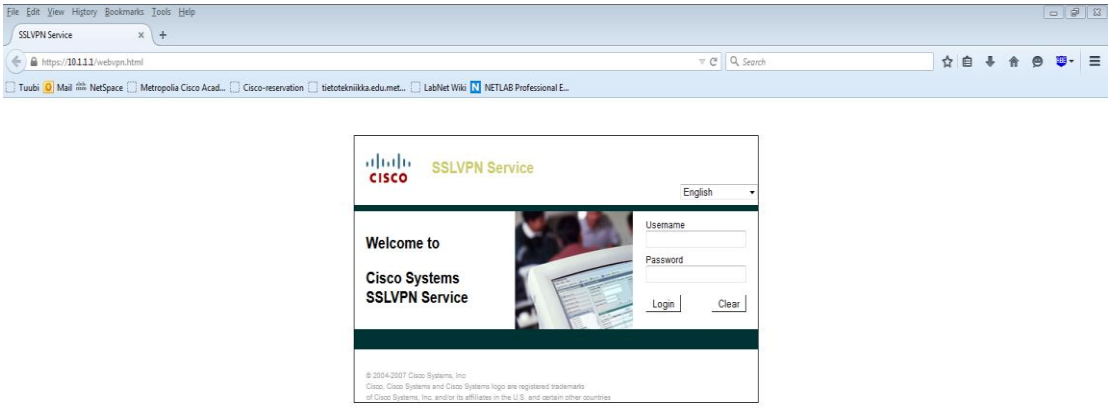
Step 24: The delivery status of the summary



Step 25: This step show the connection status

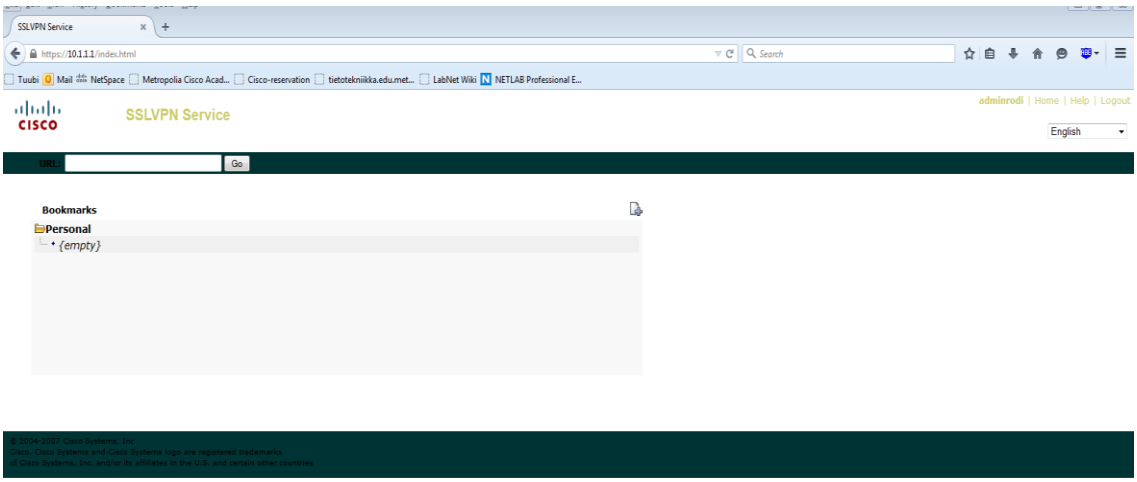


Step 26: SSL VPN login screen

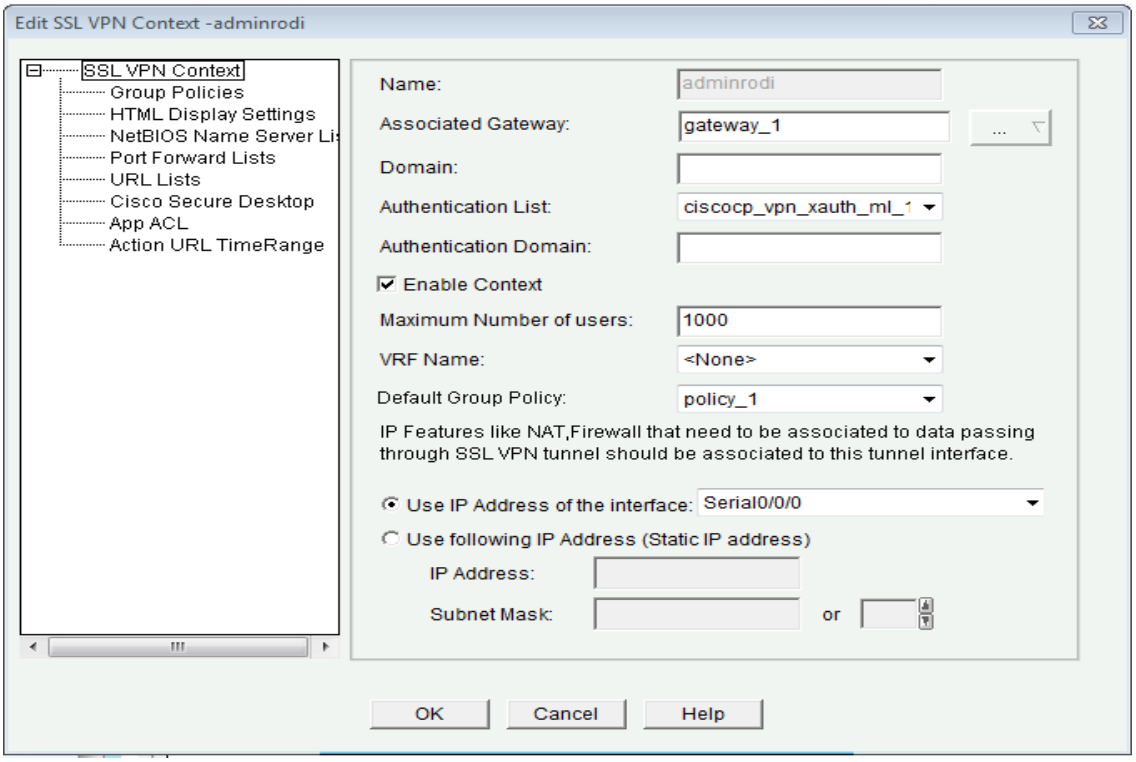


Step 27: Authenticating by using the *SSL VPN* adminrodi we created

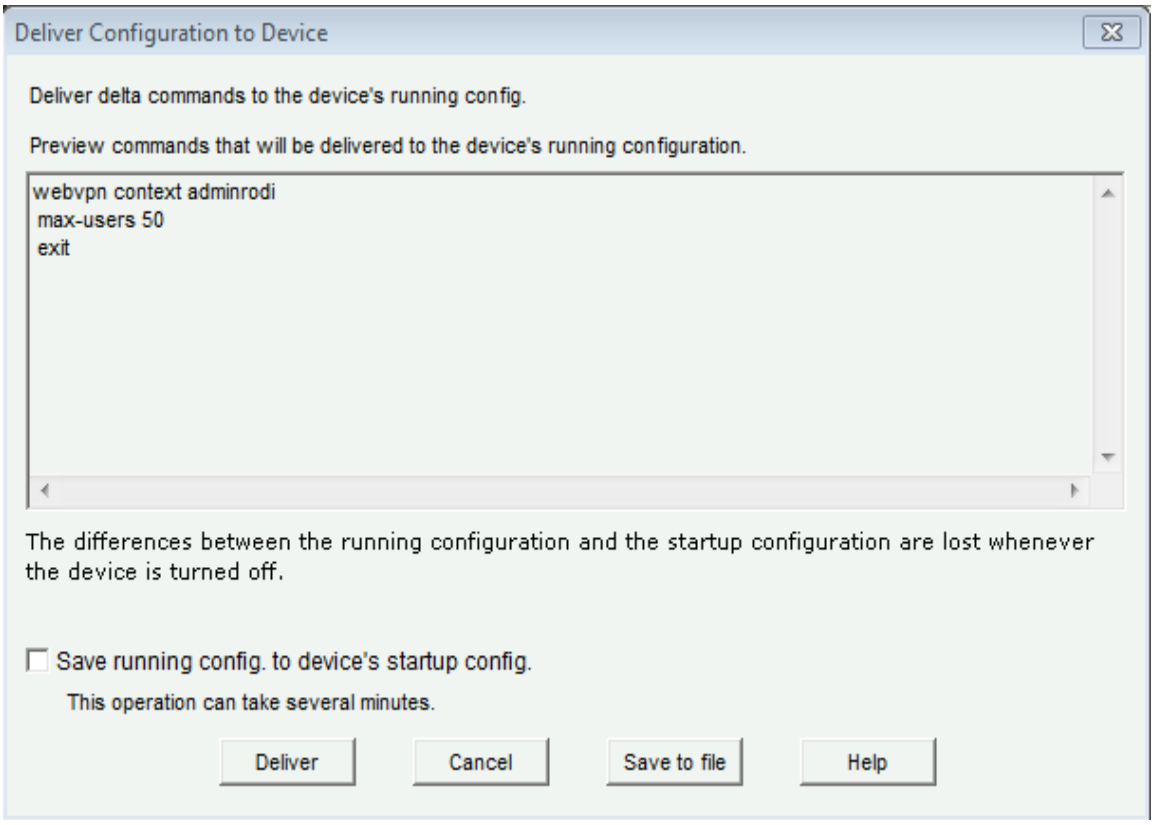
Step 28: successful authentication

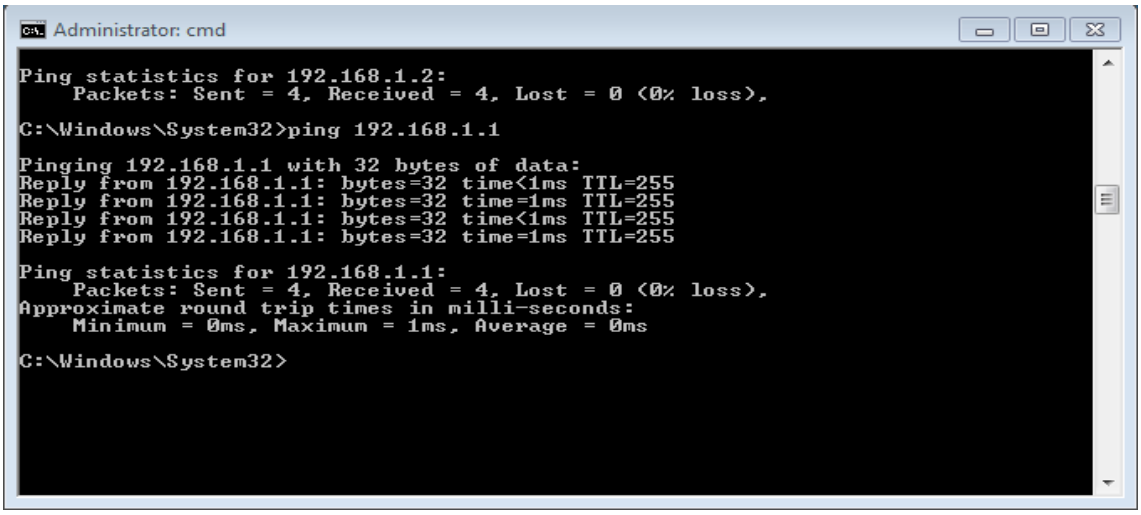


Step 29: Editing SSL VPN context



Step 30: Delivering the edited SSL VPN context




Administrator: cmd
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Windows\System32>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Windows\System32>