

Bachelor's thesis

Degree programme in Information Technology

Specialisation: Network Security

2015

A.S.M. MIR HOSSAIN

IMPLEMENTATION CONSIDERATIONS OF IPSEC VPN FOR SMALL AND MEDIUM-SIZED COMPANIES



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

Hossain Mir

IMPLEMENTATION CONSIDERATIONS OF IPSEC VPN FOR SMALL AND MEDIUM-SIZED COMPANIES

Security threats threaten online networks. The threats are targeting enterprise networks, personal networks or other networks by accessing or altering important data. Secure-less networks give authorization of access to data in a network. Network administrators need strong network security for preventing unauthorized access, misuse or modification, of the network's accessible resources.

Mostly small or medium-sized enterprises use a firewall, antivirus and anti-spam software for network security, but they are not strong enough for protecting the network. The enterprise network protection is a crucial part of network security because, the enterprise network is the most common target for hackers.

A Virtual Private Network is a reliable way to communicate between different enterprise branches and it keeps the data secure while connecting with internal networks. IPsec VPN is one of the strongest security protocols for providing data encryption and protection. It is the most secure, and reliable Virtual Private Network protocol for connecting two or more remote area networks.

The purpose of this thesis is to introduce Virtual Private Network services and implement the IPsec protocol for securing a small and medium-sized enterprise networks.

KEYWORDS:

VPN security, IPsec VPN, enterprise secure network, secure tunneling, IP networks

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS	5
1 INTRODUCTION	7
2 VIRTUAL PRIVATE NETWORK	8
2.1 Virtual Private Network (VPN)	8
2.2 Why do we need VPN?	10
2.3 OSI model and VPN	11
2.4 Types of VPN	13
2.5 Benefits of VPN	16
2.6 Practical VPN Solutions	18
2.6.1 VPN Hardware solution	18
2.6.2 VPN Software solution	19
3 IPSEC VPN	21
3.1 IPsec Structure	22
3.1.1 IPsec Mode	22
3.1.2 IPsec Protocols	24
3.2 Security Consideration	27
3.3 IPsec and TCP, IP layer	29
3.4 IPsec Architecture	30
3.4.1 IPsec Roadmap	30
3.4.2 Security Associations	31
4 IMPLEMENTING IPSEC VPN FOR SME'S	33
4.1 Host Implementation	33
4.2 Router Implementation	36
4.3 IPsec Protocol Processing	38
4.4 ICMP Processing	41
4.5 SMEs Structure and Turnover	42
4.6 IPsec Authentication	43
4.7 IPsec in Action	44
4.7.1 End-to-End Security	44
4.7.2 Network Security policies and implementation	45
4.8 Configuring site-to-site IPsec on Cisco router	47
5 CONCLUSION	50
REFERENCES	51

APPENDICES

Appendix 1. Cisco CP Configurations on Router A and B.

Appendix 2. Router B CLI Configuration

TABLES

Table 1. SMEs size and turnover in Europe	42
---	----

FIGURES

Figure 1. Example of enterprise WAN network.	9
Figure 2. An enterprise VPN connection.	9
Figure 3. The VPN protocols operate at different OSI model layers.	12
Figure 4. Remote access VPN.	14
Figure 5. Site-to-site VPN.	15
Figure 6. An IPsec tunnel mode made between two routers.	23
Figure 7. An IPsec transport mode between a server and a host	23
Figure 8. ESP encapsulates an IP packet.	24
Figure 9. Frame work of Authentication Header.	25
Figure 10. IPsec in TCP/IP network layers.	29
Figure 11. IPsec roadmap architecture.	30
Figure 12. IPsec SAs made bi-directional communications.	32
Figure 13. IPsec implementation in Bump in the Stack.	35
Figure 14. Native Implementation architecture.	36
Figure 15. Bump in the Wire implementation architecture.	37
Figure 16. An example of IPsec outbound processing.	39
Figure 17. An example of IPsec inbound processing.	40
Figure 18. End-to-end network security connection.	45
Figure 19. Network security policy and implementation system.	46
Figure 20. Site-to-site IPsec VPN between two cisco router.	49

LIST OF ABBREVIATIONS (OR) SYMBOLS

3DES	Triple Data Encryption Algorithm
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
BITS	Bump in the Stack
BITS	Bump in the Wire
CHAP	Challenge Handshake Authentication Protocol
DES	Data Encryption Standard
DOI	Domain of Interpretation
ESP	Encryption Security Protocol
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPX	Internet Protocol Exchange
IPV4	Internet Protocol Version 4
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
KLIPS	Kernel IPsec.
L2F	Layer 2 Forwarding
L2TP	Layer 2 Transport Protocol
LAN	Local Area Network
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation

OSI	Operating System
OSI	Open-Standard Interconnected
OSPF	Open Shortest Path Fast
PAP	Password Authentication Protocol
PIN	Personal Identity Number
PPP	Point-to-Point Protocol
SAs	Security Associations
SADB	Security Association Data Base
SMEs	Small and Medium-Sized Enterprises
SPI	Security Parameter Index
SPD	Security Policy Database
SPI	Security Policy Index
SSLV3	Secure Sockets Layer Version 3
TLSV1	Transport Layer Protocol Version 1
VPN	Virtual Private Network
WAN	Wide Area Network

1 INTRODUCTION

Security threats threaten personal or enterprise networks over a public area. Enterprise networks are the most common targets for hackers. Enterprise networks include organizations and personal network. Different types of tool are used for protecting enterprise networks, but they are expensive and not secure enough. Virtual Private Network (VPN) is not expensive but is a more secure way for connecting the enterprise branch or personal network in remote areas. It encrypts data by using a tunnel between two end points. In this way, it is possible to browse and transfer data safely, and securely over a public network. Small and medium-sized enterprises (SMEs) can select the VPN service for reduced costs, and trustworthy network security, rather than use the WAN (Wide Area Network) service.

VPN uses several protocols for securing virtual network connections. IPsec is one of the strongest VPN protocols for securing network connectivity. It is a suitable VPN protocol for connecting enterprise branch offices with headquarters. Because, IPsec uses a tunnel between two-end connections, the information is more secure and reliable through an IPsec VPN. The IPsec protocol is a standard for SMEs, because it does not cost much and is easy to configure. SMEs are able to configure the IPsec VPN without in-depth expertise. On the contrary, a corporation which has many employees and branches may need to hire a network engineer for configuring an IPsec VPN.

The thesis introduces VPN and, IPsec VPN and reflects on IPsec protocol implementation considerations for securing an SME network. Chapter -2 introduces VPN. Chapter -3 discusses IPsec VPN, IPsec protocol and network security matters. Chapter -4 describes an IPsec implementation for securing enterprise networks. Chapter 3 and 4 examines IPsec architecture, IPsec processing, planning network security and implementing firewalls as well as configuring an IPsec VPN on the Cisco Router.

2 VIRTUAL PRIVATE NETWORK

2.1 VPN (Virtual Private Network)

Virtual private network (VPN) is a technology used to establish a private network through a public network. It enables the employees to securely access their employer's internal network from any place, while crossing a public network. In addition, the VPN connects an enterprise headquarters and branch offices by using secure tunnels. The VPN creates a virtual network by using encryption and a tunneling protocol. In general, a corporation or enterprise uses WAN (Wide Area Network) for connecting branch offices with headquarters. WAN is expensive and the service increases when the number of sites and their interconnection sites increase. In comparison, VPN is more flexible than WAN for designing network and reducing costs. To summarize, VPN ensures secure communication by using an encrypted channel and it saves cost from around 30 to 80 percent. There are different protocols to implement VPN and the IPsec protocol is the most popular as well as one of the strong VPN for securing tunnels. (Lucas et al., 2006)

The two following figures show an enterprise WAN and VPN connectivity. The VPN connectivity saves money by using only two tunnels whereas the WAN connectivity uses a number of sites and interconnection sites that increase cost value.

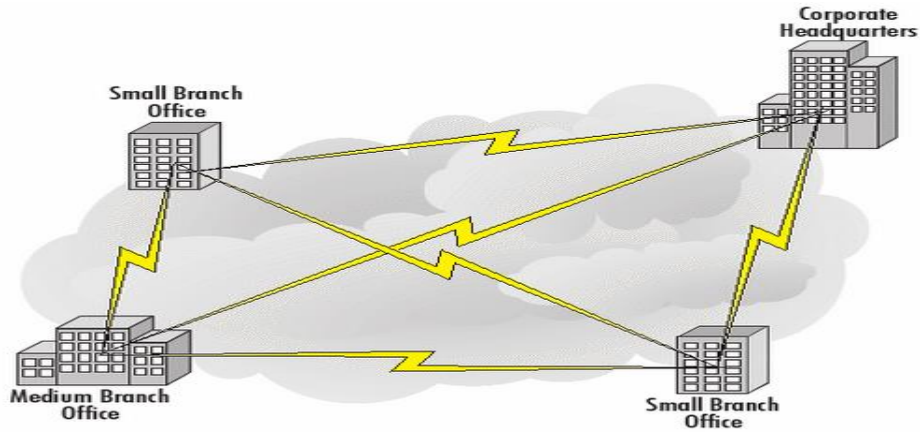


Figure 1. An example of enterprise WAN network structure between main office and branch offices. (Lucas et al., 2006)

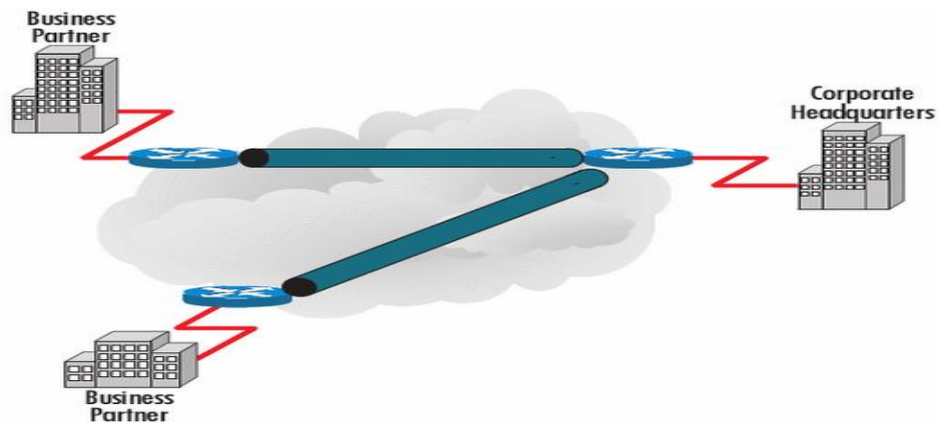


Figure 2. A VPN connection between an enterprises headquarter and branch offices (Lucas et al., 2006)

2.2 Why do we need a VPN?

A VPN is a secure and reliable communication between host and employee network. It can make a private network over the public network. A public network has more unrelated peers, so there is a possibility of leaking information during exchanges with each other. Whereas, a private network is authorized and permitted for the specific people. Those who share a private network, have agreed to use and share information only with the group members. The VPN is useful to connect with an enterprise's network while travelling with a laptop, tablet or a smart phone. A VPN client on one computer connects to another computer by using encryption and security measures, so that no one can see what information's is being transferred.

VPNs are commonly used by enterprises to connect their employees or users in remote areas. It is the best technology ever to connect remote areas at a low costs. The VPN can connect multiple geographical locations and does not use any leased lines. It gives flexibility for an enterprise to use the business intranet and it saves time and money for employees who work from remote areas. Thus, the technology uses a secure tunneling protocol and encryption, so the system is highly secure and trustable to the enterprises.

However, the VPN is not only for business use, but also can be used to access the internet anonymously. Anyone can protect their online privacy and security by using a VPN system. Different types of WANs can connect users and their organization from remote site, but they are expensive and not affordable for small companies. The VPN is cost-effective and suitable for SMEs and it gives a private network.

2.3 OSI model and VPN

OSI (Open-Standard Interconnect) is a conceptual network model in telecommunication or computer system where peer-to-peer communication is accomplished through seven layers. The VPN is a secure virtual connection system that has been developed to provide security for the OSI layer by using a different protocol. These VPN protocols work on five OSI layers except the presentation and session layers. The OSI network layer is important because the IP packets are receiving, sending, and operating from this layer. The IPsec and MPLS protocols operate at the OSI network layer. The IPsec VPN exists at OSI layer three. It is the most secure and widely used VPN and it corresponds to different layers in OSI stacking. The L2F (Layer 2 Forwarding) protocol provides tunneling for private IP address, IPX (Internet Protocol Exchange) over shared networks. The L2F protocol was developed by Cisco Systems. PPTP (point to point tunneling protocol) supports remote PPP-capable devices for integrating an enterprise network without any interruption. This protocol was created by the Microsoft Corporation. Moreover, MPLS (Multi-Protocol Label Switching) helps to transport and route several types of VPN traffic by using VPN routing.

Figure 3 shows VPN protocols operating and corresponding at different OSI layers. Although the OSI model has seven layers, the VPN protocols do not operate at presentation and session layer. The figure is a conceptual model to understand how VPN protocols work at the OSI layers. (Carmouche, 2006)

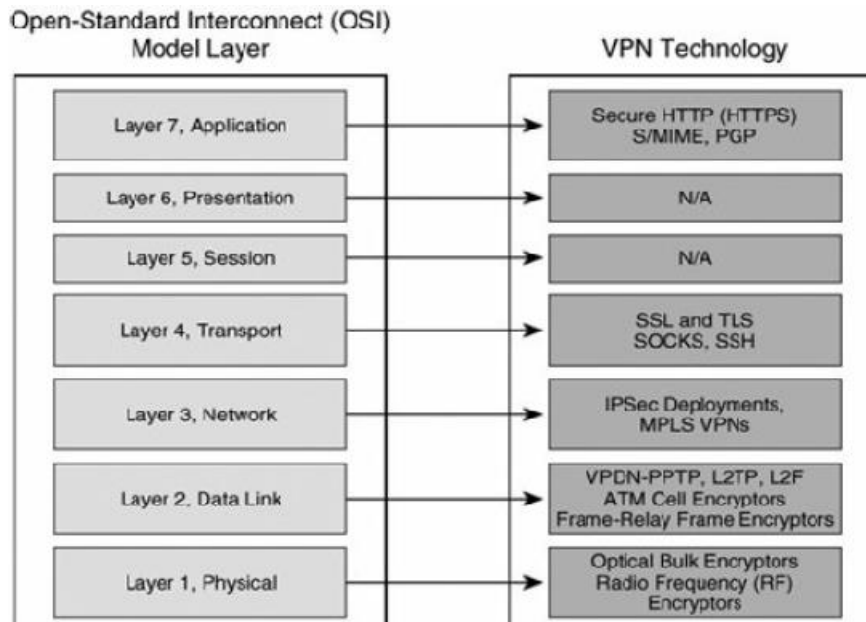


Figure 3. The VPN protocols operate at different OSI model layers.
(Carmouche, 2006)

2.4 Types of VPN

There are different types of VPN available, such as, MPLS VPN, SSL VPN, IPsec VPN, L2TP VPN, and PPTP VPN. These VPNs are commonly known as VPN protocols. On the basis of VPN service and protocol, VPN are mainly of two types: remote-access VPN and site-to-site VPN.

Remote Access VPN

Remote access VPN is a secure system to connect from remote areas to head office. Users who access the information in the network, must be connected in the network's access server. A large enterprise which has more sales person in remote areas needs a remote access VPN. Two types of components are used for a making a remote access VPN, NAS (Network Access Server) which is known as media gateway and client software. The NAS is responsible for providing valid credentials to the users that operates to sign in to the VPN. It uses an authentication process for checking the valid users. However, it is possible to connect to the enterprise's network from an individual computer by using a VPN. However, the employee must set-up a VPN client software on their computer. The client software makes a tunnel connection to the network access server and keep the connection secure. (Tyson & Crawford, 2011)

Figure 4 shows, a remote user connected with main office by using a remote-access VPN. The remote user is connected with a network access server in front of a head office that provides a connection between the two networks.

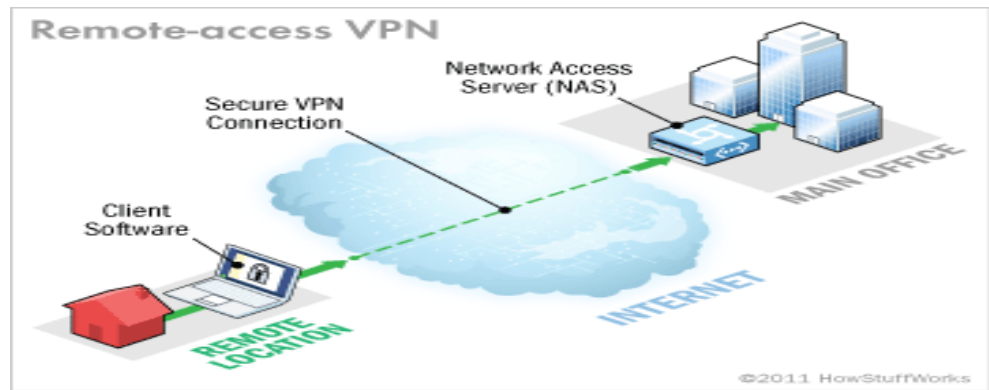


Figure 4. A remote access VPN created between a remote user and a head office. (Source: <http://computer.howstuffworks.com/vpn3.htm>)

Site-to-Site VPN

A site-to-site VPN uses several offices in different locations for securing a connection over the internet. The site-to-site VPN provides computer resources available for all user connected to the network. A growing enterprise which has several branch offices in different locations needs a site-to-site VPN connection. The site-to-site VPN can be, Intranet-based or Extranet-based.

Intranet-based: A company which has at least one remote location may use a single private network. The company needs to create an intranet VPN for connecting each separate LAN (Local Area Network).

Extranet-based: An existing company may have a relationship or partnership with other companies, customers, and suppliers. When those companies' LANs are connected with each other, they can build an extranet VPN. (Tyson & Crawford, 2011)

Figure 5 shows several of branch offices of an enterprise connected using site-to-site VPN connection. The branch offices are connecting with a network access server in front of the head office that provides connection among the branch networks.

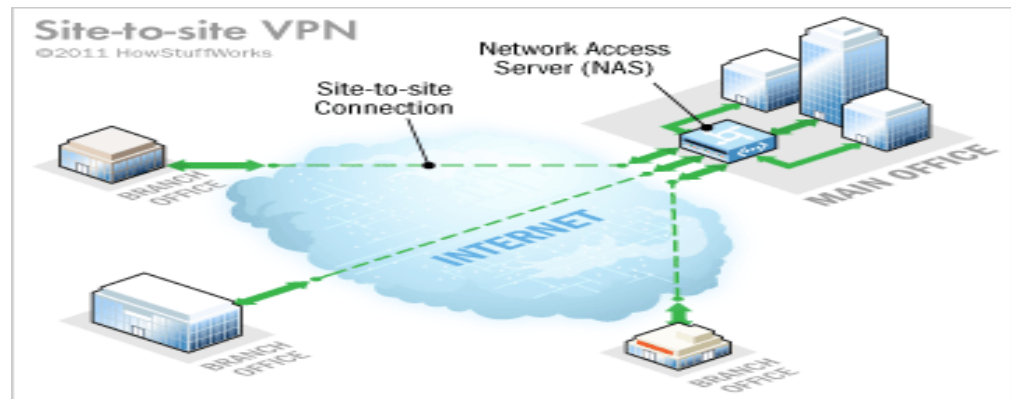


Figure 5. A site-to-site VPN created among three branch offices and a head office. (Source: <http://computer.howstuffworks.com/vpn4.htm>)

2.5 Benefits of VPN

The VPN provides great value to the enterprise. It provides cost saving, scalability and enhances communication security and reliability.

Cost Savings

Money is the most important asset in all businesses. The VPN saves a great amount of money than traditional or high cost technologies. The VPN became popular because, its remote access service gives remote user authentication. The remote access service was expensive and difficult to scale using modem pools. Then the VPN arrived and supported a large number of remote access capabilities during the early age of broadband internet. The VPN gained popularity for offering better performance, low cost, and high speed internet access. The VPN can be used as a WAN link that saves money and helps to cover basic WAN costs.

Scalability

Scalability of VPN is extremely good compared with other technologies. To scale a VPN, we need to design a network, analyse product performance history and capabilities. A new user or a group can simply be added to an existing client package in a remote VPN solution system. A traditional dial-up system, needs extra equipment and phone lines to increase the size of a network, whereas the VPN access device needs more processor speed and memory. In addition, the traditional remote access solution were more expensive than VPN. For that reason, the entry cost of expandability becomes a great issue between traditional remote access solution and VPN. (Tiller, 2000)

Enhance Communication Security

At the beginning of VPN technology, the communication system were not strong and it was easy to attack a network. The information shared on a private network was not encrypted. When the VPN was implemented, the protection

control of internet communication was removed from the application and user level to the network level because the VPN technology does not make any troubles to an existing program and operator as well as it provides data confidentiality. At the moment, the internet protocols using VPN are stronger for securing communication over the public network. (Tiller, 2000)

Reliability

The remote user is able to connect the enterprise network at any time by using a VPN. It can provide equal connections for each user. Nowadays, there is a new broadband VPN system that offers high bandwidth and better network reliability in reasonable price. (Tyson & Crawford, 2011)

2.6 Practical VPN Solutions

VPN technology is used in the telecommunication and wireless sector. Mobile worker living in remote location use VPN for accessing data securely. Since the workers are travelling to many places and use wireless internet, the internet access is vulnerable and it is easy to attack their network traffic. A standard VPN solution connects the remote user securely with his/her main office without using private leased lines. The VPN can be implemented in a network by using hardware or software services. (Lucas et al., 2006)

2.6.1 VPN Hardware Solution

There is a myth that a hardware VPN can provide stronger security than software. However, a VPN device supports high performance and it is easy to set up with an existing network. There are two types of VPN devices, stand-alone and multifunction devices. Stand-alone VPN devices have a higher data transfer rate than the multifunction devices. In addition, the stand-alone devices have multiple authentication protocols such as RADIUS, LDAP and Active Directory. While the multifunction devices may support limited protocols, the stand-alone VPN devices are expensive and are using by the medium or large enterprises whereas the multifunction devices are cost effective and used by small companies.

VPN devices may run on their own operating system. It is possible to run these devices on Windows and Linux operating systems. Different types of VPN devices are available on the market and these are made by several renowned networking companies. VPN hardware devices include

Juniper SSL VPN

Juniper Network Secure Access is a popular VPN in the market. It is based on an instant virtual extranet platform and it uses a secure socket layer protocol. The Juniper Secure Access devices 700, 2000 are used for small and medium sized enterprises. (Lucas et al., 2006)

SonicWALL

SonicWALL has two types of VPN such as, SSL-VPN 2000 and SSL-VPN 200. The SSL-VPN 2000 is for enterprise which have around 1000 or fewer employees. On the other hand, the SSL-VPN 200 is for the enterprises which have almost 50 or fewer employees. (Lucas et al., 2006)

Cisco IOS VPN, Cisco Easy VPN

Cisco IOS VPN gives flexibility in VPN design. It supports a diverse networking environment, reliable delivery of latency sensitive traffic, VPN scalability and management framework. In addition, Cisco Easy VPN provides consistent VPN policies and key management methods, so it is reliable for remote areas VPN service. Cisco Easy VPN remote service supports Cisco IOS router and Cisco IPX firewall to act as remote VPN clients.

(Lucas et al., 2006)

2.6.2 VPN Software Solution

Software-based VPN is cheaper and can be compared with Hardware-based VPN. The functions are same in both VPN systems. The VPN software solution is a slightly more complicated than the VPN hardware solution. By choosing VPN software, its owner is responsible for patching the operating system and VPN components. Additional software' running on an operating system may need to be patched because, when these applications running on an operating system, they can listen for incoming traffic on ports.

There are various types of open-source and commercial VPN software existing on the market. Some examples are given below:

Openswan

Openswan is a Linux OS based free software developed for the IPsec implementation. It has three VPN divisions. The first division is KLIPS (Kernel IPsec) that provides encryption and authentication. The second division is IKE (Internet Key Exchange) daemon that connects IKE with other systems. The

third division is a combination of different scripts which provides an admin interface. More information about Openswan is available on the official Openswan website. (Lucas et al., 2006)

Microsoft

Microsoft has developed VPN services for the Windows operating system. It is a commercial service and based on IPsec and L2TP (Layer 2 Transport Protocol). Users must know the Microsoft PKI (Public Key Infrastructure) in order to run the VPN. In addition, the user need to be trained to connect to the Microsoft VPN solution.

(Lucas et al., 2006)

Open VPN

OpenVPN is a popular open-source software developed by James Yonan. The software supports VPN for connecting point-to-point or site-to-site network securely. It uses a pre-shared secret key, certificate, username and password for peer authentication. The OpenVPN can apply to multi-client and it provides authentication for every client. It uses SSLv3 (Secure Sockets Layer) or the TLSv1 (Transport Layer Protocol) protocol and encryption system.

3 IPSEC VPN

IPsec is a security scheme for intercommunicating with two authorized networks from different locations. The IPsec is built for secret communication and is reliable over the IP network by using authentic and cryptographic security services. It uses a framework to secure information, so that the data sent through the IPsec have data integrity and data confidentiality. IPsec VPN ensures peer-to-peer data security by using encryption. It is the most popular VPN technologies for securing an enterprise, personal, or government network. The IPsec VPN protects network vulnerabilities by using several layers of protection. It can protect and authenticate an IP packet by using several protocols like ESP, AH and IKE. Normally, the IPsec is used for checking data integrity, data confidentiality and the data origin authentication between two hosts at the TCP/IP's network layer. The IPsec VPN ensures a secure path between two host's nodes or two gateways nodes as well as it can make a secure path between a gateway and a host.

IPsec History

In 1993, a case about IP Layer security was submitted by two men from Columbia University and Bell laboratories. The case demonstrated how to implement security features without changing the IP structure. It was extended by using authentication, encapsulation and transparency. The case was crucial to IP security and it was combined with existing security weakness of IP protocols. In 1994, IAB (the Internet Architecture Board) stated that a group of people demanded for internet security and the case was important for the IPsec protocol. (Tiller, 2000).

3.1 IPsec Structure

IPsec requires four key elements for enabling a strong VPN. Those elements are security protocols, key exchange mechanisms, algorithms for encryption and secure key exchange, SAs (security associations) definition and maintenance. In addition, the IPsec has two modes for securing communication, transport mode and tunnel mode. It has two standard protocols known as Encapsulation Security Protocol (ESP), Authentication Header (AH). (Carmouche, 2006)

3.1.1 IPsec Mode

IPsec modes are mainly of two types: Tunnel mode and Transport mode.

Tunnel mode

In tunnel mode, a secure tunnel is made between two routers or firewall gateways. The gateway is responsible for delivering data to the host. By using tunnel mode, IPsec is able to encrypt the IP header and the payload. On the opposite, the IPsec transfer mode can only encrypt the IP payload. The tunnel mode gives full security to an IP packet by using IPsec ESP protocol and it can protect the traffic between different networks. The tunnel mode works on the gateway to gateway, server to gateway and server to server configurations. (TechNet Microsoft Library, 2005)

Figure 6 shows an IPsec encrypted tunnel mode made between two Cisco routers. Thus, the user on network 20.20.20.0 /24 could browse the network 10.10.10.0 /24 in a secure and safe way. In this case, the IPsec VPN has been created between the router gateways.

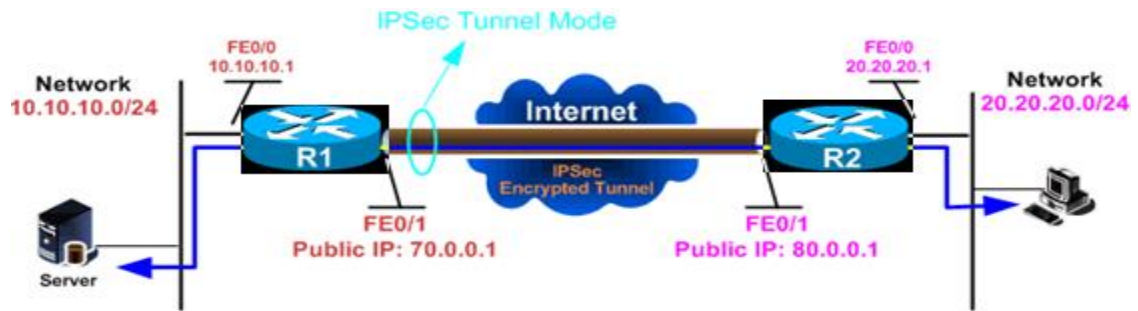


Figure 6. An IPsec tunnel mode made between two routers over the public internet. (Source:<http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>)

Transport Mode

The transport mode is enabled by default in IPsec mode. In transport mode, the host and other end device communicate directly. Although the IPsec protocol cannot encrypt the IP header, it encrypts the IP payload. (TechNet Microsoft Library, 2005)

Figure 7 shows an encrypted telnet made between a server and a host. In this case, the IPsec VPN created by the server and host end points directly. The information is being transferred between the network 140.0.0.1 and 94.200.5.5 are encrypted by the IPsec encryption tunnel.



Figure 7. An IPsec transport mode created between a server and host over the public internet. (Source:<http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>)

3.1.2 IPsec protocols

IPsec consists of three key protocols namely ESP, AH and IKE.

ESP

ESP (Encapsulation Security Protocol) secures the IP packet by providing different security services. The services provided by ESP include data authentication, data integrity, data and data flow confidentiality. ESP uses DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard) for providing data confidentiality. The ESP protocol can be used either in transport or tunnel mode.

Figure 8 shows that the header part placed before ciphered at the transport mode, as a result the ESP provides only data confidentiality. In tunnel mode, the ESP header has been placed between the chipped inner IP and the outer IP header. So, the IP traffic flows running between the source and destination are protected by IPsec tunnel mode. (Carmouche, 2006)

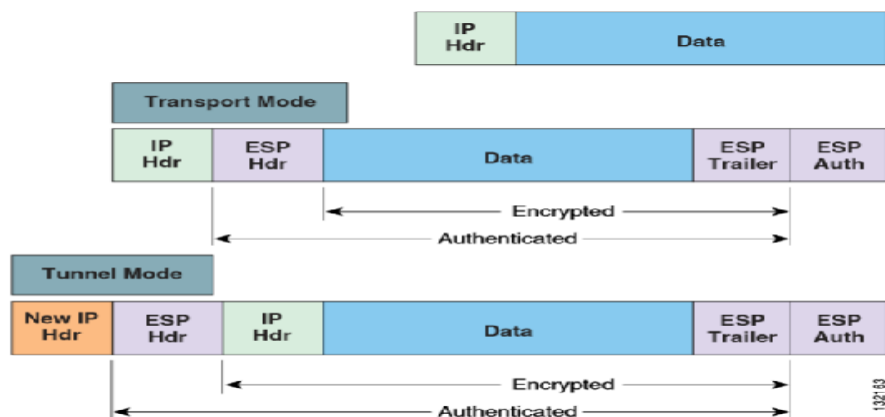


Figure 8. A structure of how the IPsec protocol ESP encapsulates an IP packet. (Sources: https://www.cisco.com/application/pdf/en/us/guest/netso/ns171/c649/ccmigration_09186a008074f22f.pdf).

AH

AH (Authentication Header) gives the data authenticity and provides integrity services for the IP packet. The header cannot encrypt the data, but it keeps it hidden by using a tamper-evident seal. For this reason, the data provided through IPsec AH is not confidential. (Carmouche, 2006)

The authentication header uses the slide window technique and discards old IP packets to protect the network from a replay attack. Figure 9 shows an AH packet construction and interpretation. The AH packet formation has been described broadly in the diagram.

Authentication Header format																																	
Offsets	Octet ₁₆	0								1								2								3							
Octet ₁₆	Bit ₁₀	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Next Header								Payload Len								Reserved															
4	32	Security Parameters Index (SPI)																															
8	64	Sequence Number																															
C	96	Integrity Check Value (ICV)																															
...																															

Figure 9. AH (Authentication Header) packet construction and interpretation. (Source: <http://en.wikipedia.org/wiki/IPsec>)

Next Header (8 bits)

The next header shows upper layer protocol protection. It uses the first 8 bits from the list of IP protocol numbers.

Payload Len (8 bits)

It measures the authentication header length. The length is 32 bit units, minus 2.

Reserved (16 bits)

This header is reserved for using in the near future.

Security Parameter Index (32 bits)

This thirty-two bits use to identify receiver security associations.

Sequence Number (32 bits)

The sequence number (32 bits) prevents replay attacks.

Integrity Check Value (multiple 32 bits)

This header is used for checking variable length value. It contains padding by putting 8 octets and 4 octet's boundary for IPV6 and IPV4.

(Source: <http://en.wikipedia.org/wiki/IPsec>)

IKE

IKE (Internet Key Exchange) is an IPsec protocol used to set up the security associations. It gains authenticated keying material for the security services such as AH and ESP. The purpose of IKE is to create security parameters and authentication keys between the IPsec peers. IKE is a mixture protocol from the Oakley and SKEME protocols, and it operates inside the ISAKMP (Internet Security Association Key Management Protocol) framework. The IKE uses several authentication methods, namely: pre shared keys; digital signature standard; digital signature using an RSA key algorithm; and revised method of authentication. (Doraswamy & Harkins, 1999)

IKE provides several benefits:

- a. IKE allows dynamic authentication.
- b. It allows encryption keys to change in IPsec sessions.
- c. It provides anti-replay services for IPsec.

3.2 Security Considerations

No security exists for the IP packets by default. So it is risky to send an IP packet through a public network because the IP packet might be changed or altered by someone in the network. Therefore, several IP protocols are used to encrypt and authenticate which ensures that an IP packet originates from the original sender. The IPsec is a standard protocol which is strong, and extensible that gives security to TCP or UDPs upper layer protocols and safe the IP packet. (Doraswamy & Harkins, 1999)

Authentication

Authentication is used to give access to the right person. It is a system to determine the identity of users who match the same security requirements. The formula of authentication is that the user has privileges to access something from others or it knows the other user already. Authentication is achieved by implementing several factors known as one, two or three. In factor two authentication, the user knows its username and password and they are given a token number which is known as PIN (Personal Identity Number) number. The PIN number is used to verify the user with the password and username given. The IPsec VPN uses factor two authentication by using CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authenticate Protocol) for remote access. However, there are other authentication systems based on physical attributes which is known as biometrics. (Tiller, 2000)

Access Control

Access control restricts access to a network. An access control list allows or denies an IP packet from outside of the network. ACL (Access Control List) accepts IP traffic from the authorized network. An example is,

```
Permit IP 147.151.77.0 0.0.0.255 host 194.72.6.205
```

The given example allows IP traffic from the network 147.151.77.0 and delivers it to the specific host IP address, 194.72.6.205. The access control can uniquely

identify an activity or process by using different attribute. Additionally, the IPsec protocol has selector properties to limit the communications when using a VPN. (Tiller, 2000)

Data Integrity

The meaning of data integrity is to provide the data accuracy and consistency from storage to end user. In general, the data has three preliminary stages,

1. Data storage
2. Data processing
3. Data transmission

Data storage and data transmission are crucial stages for protecting the data. Data storage faces several attacks like, excessive privileges, SQL injection, Denial of Service and weak authentication. In addition, when the data travels from storage to end user, it uses a public network which is untrusted and vulnerable. There is a possibility of unwanted interaction in the network, so the data could be modified or deleted when the participants are unknown. The TCP/IP protocol supports checksum process fingerprint, so the receiver can identify that the data has not been modified or altered on the public network. The IPsec uses message authentication processes, which is known as the HASH algorithm that produces a message fingerprint. (Tiller, 2000)

3.3 IPsec and TCP/IP layer

IPsec operates at the TCP/IP's network layer. IPsec provides services to the upper layers and it has no impact there. Similarly, the protocol has no effect on providing connectivity on the lower layers. To implement IPsec on a communication stream, there is no need to modify the applications or appliances. When data reaches the network layer, the VPN decides whether to implement the IPsec or not. Furthermore, when the IPsec inner part is revealed, the outside part between the layer and the operation is hidden. For that reason, the IPsec application process totally remains unaware of lower layer aspects by using a VPN. In fact, the VPN may need to deal according to the upper layer demand. Integrating the IPsec process into an existing TCP/IP's network layer makes a huge change in the protocol stack. (Tiller, 2000)

Figure 10 shows how the IPsec protocol works at TCP/IP's network layer and operates with the application layer.

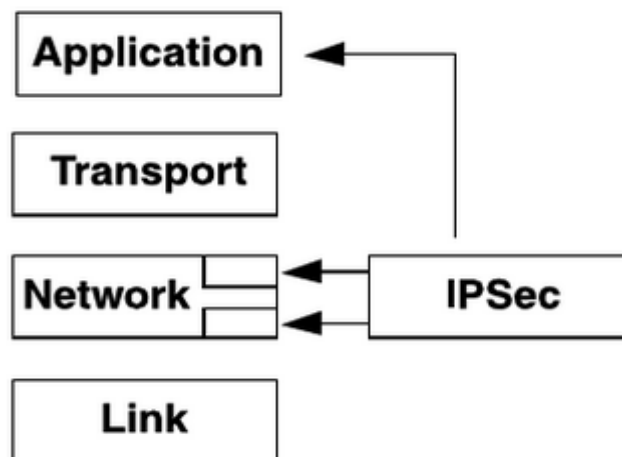


Figure 10. IPsec protocol operates in TCP/IP network layers. (Tiller, 2000)

3.4 IPsec Architecture

The IPsec architecture includes different type of IPsec components, protocols, modes and operations.

3.4.1 IPsec Roadmap

IPsec has several protocols such as ESP, AH, IKE (Internet Key Exchange), ISAKMP (Internet Security Association and Key Management Protocol) /Oakley and transforms. The IPsec roadmap describes how the different component of IPsec communicate with each other. The ESP provides data confidentiality by using encryption and encapsulation. In addition, the AH deals with the payload header format and packet structure. Moreover, the IKE produces key for the IPsec protocols. The IKE payload also negotiates keys for other running protocols in internet such as the OSPF (Open Shortest Path Fast) protocol. (Doraswamy & Harkins, 1999)

Figure 11 show, a roadmap architecture for different IPsec protocol like, ESP, AH and key management. It illustrates the encryption and authentication algorithm, policy as well as the key management system of ESP and AH.

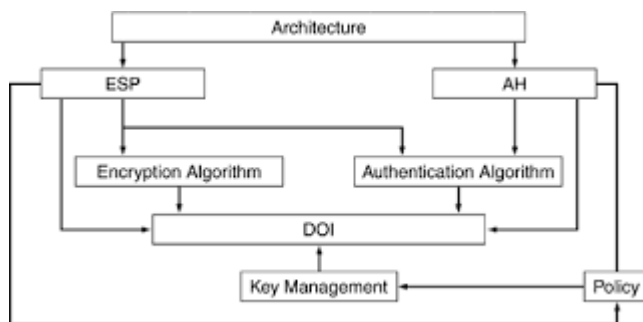


Figure 11. An IPsec roadmap architecture for IPsec protocols, policy and key management. (Doraswamy & Harkins, 1999)

Encryption Algorithm and Authentication Algorithm

The encryption algorithm is used by ESP for enforcing data confidentiality. It is a set of transformation that includes document key size, key generation and mechanism. However, the authentication algorithm is used by AH and ESP's authentication option. (Ganguly, 2012)

DOI and Key Management

DOI (Domain of Interpretation) describes an exchange type, operational parameter and payload format. The key management is a set of guideline that describes key management system. (Ganguly, 2012)

Policy

The policy is an important component in IPsec architecture. It determines transform to use entity communications. (Doraswamy & Harkins, 1999)

3.4.2 Security Associations

The SAs (Security Associations) make a legal agreement between two entities. Security Associations are based on two basic forms in an IPsec VPN.

IKE Security Associations

The IKE (Internet Key Exchange) has duplex mode. This means that a single IKE can communicate between two systems. By establishing a VPN, the IKE allows communication terms and conditions to authenticate and connect properties. While the two systems are connected to whom they desired, SAs is established for conducting information. When authentication is managed and the keys are created, the information can be encrypted, because of the SAs have been created. (Tiller, 2000)

IPsec Security Associations

In IPsec SAs, two Security Associations (SAs) are recommended for using bidirectional communication between two systems. Two SAs provide data confidentiality and strong authentication.

Figure 12 shows how the data transmission is protected by using two IPsec SAs. When using two Security Associations (SAs), the data transfer is stronger and confidential.

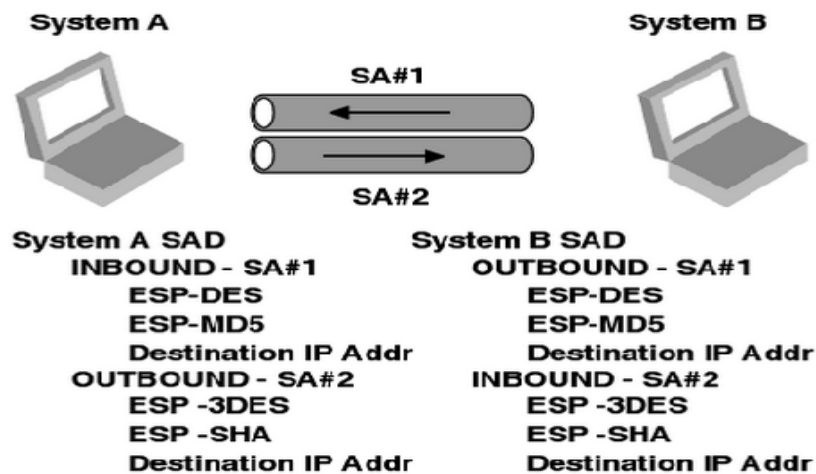


Figure 12. The IPsec SAs bi-directional communication between two hosts. (Tiller, 2000)

When using two SAs, one is protecting inbound and other is protecting outbound data traffic on each system. So the data is confidential and protected through the IPsec SAs process.

IPsec SAs has three components:

1. Security Parameter Index (SPI)
2. Destination IP address
3. Security protocol identifier.

(Tiller, 2000)

4 IMPLEMENTING IPSEC VPN FOR SMES

In general, the IPsec is implemented on host gateways/routers or in end-to-end hosts. The following section describes the IPsec integration with the OS (Operating System), IPsec protocol processing and its implementation of different network devices.

4.1 Host Implementation

The host device is where the IP packets originate. There are some advantages in implementing a host device:

- a. The host provides end-to-end security.
- b. The host provides security continuity.
- c. The host has the ability to implement all IPsec modes.
- d. It can maintain a user context for IPsec authentication.

The IPsec host implementation is carried out in two ways. The first one is implementation with OS and which is known as OS Integrated. The second one is implementation with network layer and data link layer, which is known as “Bump in the Stack”. (Doraswamy & Harkins, 1999)

OS (Operating System) Integration

The IPsec allows integration with OS within the host implementation system. As part of the network layer protocol, IPsec is implemented on this layer. The IPsec layer uses the service from the IP layer to build the IP header. There are some benefits of integrating the IPsec with OS. Those benefits are listed below:

1. If the IPsec is firmly integrated with the network layer, it can be used for network services such as user context, fragmentation and PMTU.
2. When integrating IPsec with OS, it supports all IPsec modes.

3. By integrating IPsec with OS, the security services goes smoothly per flow, such as a web transaction. The security services can be provided as the key management and IPsec protocol. The integration between the network layer and IPsec happens seamlessly. (Doraswamy & Harkins, 1999)

Bump in the Stack (BITS)

Operating System (OS) integration is not suitable solutions for the VPN and intranets because the OS vendor sends features to the end hosts. So, that might be an obstacle to providing advanced VPN solutions. To reduce the problem, the IPsec is used as a shim between the TCP/IP's data link and network layer. The system is commonly known as BITS (Bump in the Stack) implementation. (Doraswamy & Harkins, 1999)

In this BITS scenario, IPsec makes a new layer between the data link layer and IP layer. It is placed in the networking protocol self as an extra element. By using BITS IPsec implementation, it makes an individual layer in the TCP/IP stack. The implementation setup takes place under the IP layer and it includes security by creating an IP layer. BITS are normally used in IPV4 (Internet Protocol Version 4) hosts.

The following figure describes how the IPsec has made a separate layer between the IP and the network layer. In addition, the IPsec protocol manages the security protection for an IP packet from the IP layer. The figure illustrates an IPsec Bump in the Stack architecture.

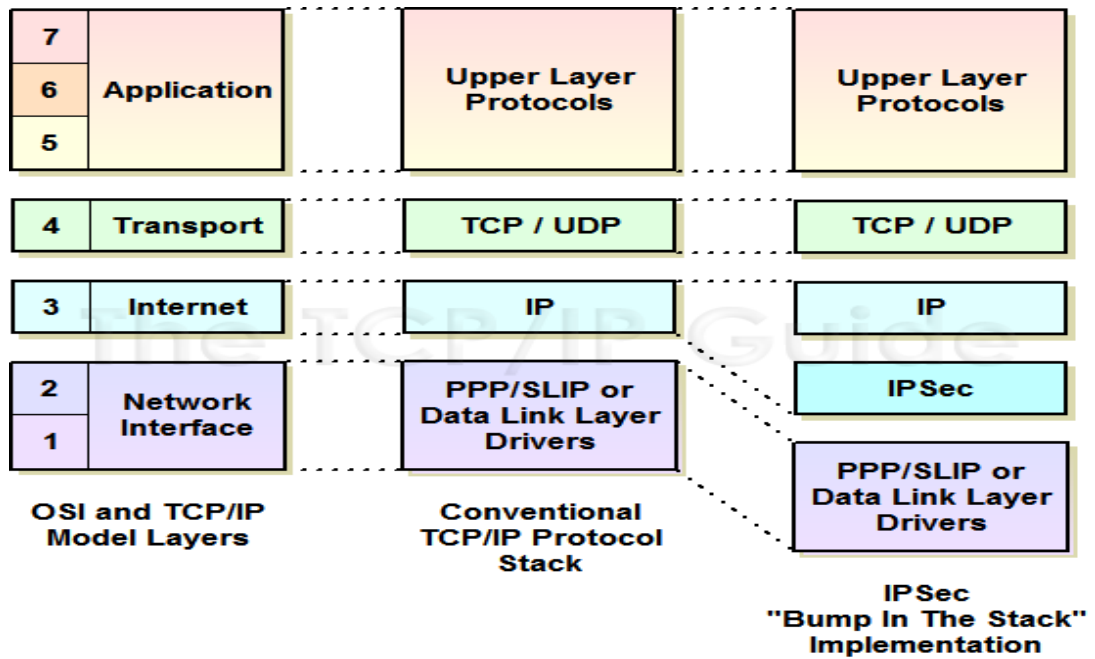


Figure 13. IPsec implementation in BITS (Bump in the Stack) architecture.
 (Source: http://www.tcpipguide.com/free/t_IPSecArchitecturesandImplementationMethods-2.htm#Figure_117)

4.2 Router Implementation

The IPsec implementation on a router ensures the IP packet security over a part of a network. By using IPsec authentication and authorization, the router restricts users from entering the private network.

Router implementation is of two types: Native implementation and Bump in the Wire (BITW). (Doraswamy & Harkins, 1999)

Native Implementation:

In native implementation, IPsec is implemented in a router software. So, there is no need to put the extra IPsec device on the router's physical interface. The following figure shows two routers connected by using native implementation IPsec. (Doraswamy & Harkins, 1999)

Figure14 shows that the routers A and B are connected by using a native Implementation system that uses a VPN software to connect the routers A and B instead of a VPN appliance.

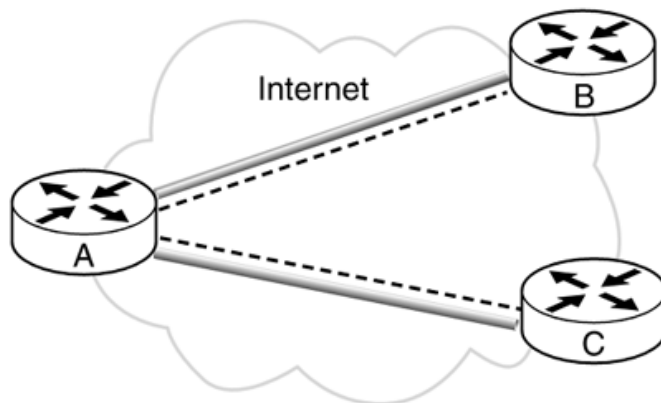


Figure 14. A native Implementation architecture among the three routers over the public network. (Doraswamy & Harkins, 1999)

Bump in the Wire (BITW)

In BITW implementation, IPsec is implemented in an IPsec device. The device connects with the router physical interface. It secures IP packets coming from outside of the network. The following BITW (Bump in the Wire) architecture describes that an IPsec device has been implemented at router port RA_B to router RB. So the device authenticating and authorizing IP packets comes from router RB. (Doraswamy & Harkins, 1999)

In Figure 15 the routers A, B are connected by using Bump in the Wire Implementation. AVPN hardware device on router A is used to connect the routers A and B rather than a VPN software.

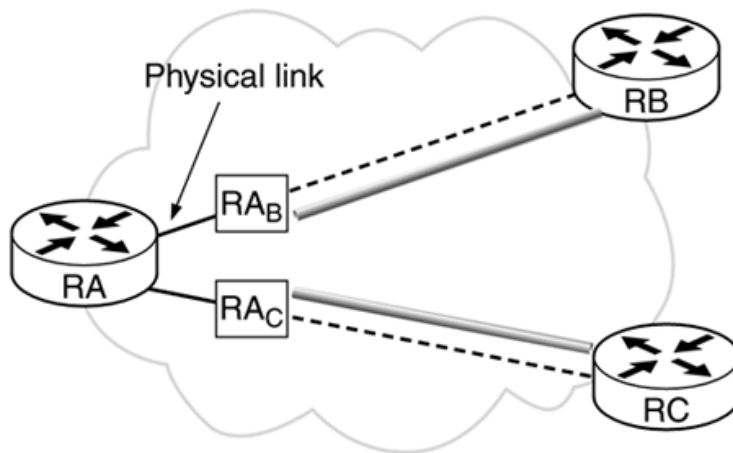


Figure 15. BITW (Bump in the Wire) Implementation architecture among three routers over public network. (Doraswamy & Harkins, 1999)

4.3 IPsec Protocol Processing

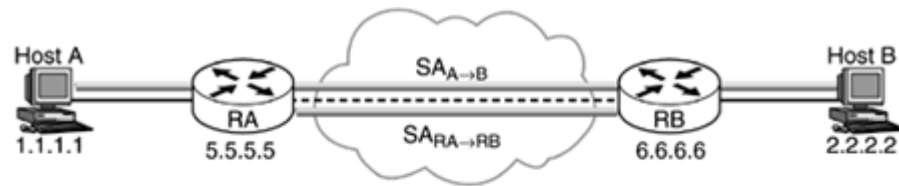
The IPsec has several types of protocol and they are different from each other. The IPsec processing is mainly divided into two parts, such as inbound versus outbound processing and ESP versus AH. Further, the protocol processing can be divided into SA (Security Association) processing, SPD (Security Policy Database), transform processing and header. The outbound and inbound processing are described in this section.

Outbound Processing

In general, the TCP/IP's transport layer communicates with IP layer to send a packet by using a function named `ip_output`. The function has a parameter that uses a source address and the destination address to enable the IP layers, which build the IP header. In addition, the transport layer passes a protocol value from the header field. SPD (Security Policy Database) processing decides whether the IP packet security can enter the `ip_output` function. (Doraswamy & Harkins, 1999)

In the following diagram, the router interface exposes the public network. Since, the outbound processing has been described here, an HTTP packet is being sent from host A to host B by using routers RA and RB interface. The purpose of the SPD policy on host A is to give authorization of AH (Authentication Header) to host B in transport mode by using HMAC-MD5 keys. In addition, the purpose of policy on router RA is to give authorization of all IP packets to the network 2.2.2 /24 on router RB. The IP packets are being sent through the tunnel are using ESP encryption and with 3DES (Triple Data Encryption Algorithm).

(Doraswamy & Harkins, 1999)



A's SPD

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	Any	Any	Transport AH with HMAC MD5

A's Outbound SADB

Src	Dst	Protocol	SPI	SA record
1.1.1.1	2.2.2.2	AH	10	MD5 key

$SA_{A \rightarrow B}$

From	To	Protocol	Port	Policy	Tunnel dst
1.1.1/24	2.2.2/24	Any	Any	Tunnel ESP with 3DES	6.6.6.6

RA's Outbound SADB

Src	Dst	Protocol	SPI	SA record
5.5.5.5	6.6.6.6	ESP tunnel	11	168-bit 3DES key

$SA_{RA \rightarrow RB}$

Figure 16. An example of IPsec outbound processing between two hosts and two routers. (Doraswamy & Harkins, 1999)

Inbound Processing

Inbound Processing is less complex than outbound processing. It only checks the header and does not interact with key management system. The AH and ESP processing on inbound processing are almost same as the outbound processing except for the transform and header processing. Layer 2 uses the IP layer to process the IP packets that are sent from interfaces. At the beginning of the process, the IP layer removes the IP header and uses the IPsec layer with the AH/ESP header.

The outbound processing network diagram illustrated in Figure 18 is considered here. In Figure 19, the SADB (Security Association Data Base) and SPD are implemented for inbound processing.

In the following inbound processing framework, a tunnel process operates between router RB and RA. The router RB receives an IP packet from router RA source 5.5.5.5. It uses ESP tunneling by using 3DES keys with SPI (Security Policy Index) value 11. In addition, the host B and host A will be the part of the inner IP header. The two hosts use the AH protocol with HMACDMD5 keys for connecting. SPD (Security Policy Database) matches the network 1.1.1 /24 from 2.2.2 /24.

(Doraswamy & Harkins, 1999)

RB's SPD

From	To	Protocol	Port	Policy	Tunnel entry
2.2.2/24	1.1.1/24	Any	Any	3 DES EPS	5.5.5.5

RB's Inbound SADB

Source	Destination	Protocol	SPI	SA record
5.5.5.5	6.6.6.6	ESP	11	168-bit 3DES key

B's SPD

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	AH	Any	Transport AH with HMACDMD5

B's Inbound SADB

Source	Destination	Protocol	SPI	SA record
1.1.1.1	2.2.2.2	AH	10	HMACDMD5 key

Figure 17. An example of IPsec inbound processing. (Doraswamy & Harkins, 1999)

4.4 ICMP Processing

ICMP (Internet Control Message Protocol) is part of Internet Protocols used by routers or equivalent networking devices to send error message notification. It can be used for query messages. The ICMP error and query messages are used for checking network status. The ICMP error messages are created by end hosts and work as normal IP packets. In addition, the origin and destination routers communicate with each other by creating tunnel mode SA. The SAs (Security Associations) are responsible for sending ICMP error messages. (Doraswamy & Harkins, 1999)

However, the ICMP messages have two kinds of structure, one-octet type field and two-octet type checksum. The one octet type field explains what types of functions are filing the message and checks the content of the messages. The two-octet type checksum uses code fields. Its content includes the ICMP message header and first eight octets which send error message notifications. (Loshin, 2003)

4.5 SMEs structure and turnover

There are different explanations of SMEs structure and turnover. Normally, SMEs are organized into client section, business section, and management section. SMEs are mainly led by the management section, where there is a director and all the employees' work as subordinates. According to European Commission, SMEs employees are between 50-250 people and their annual turnover ranges between 10-50 million euros.

Table 1. SME's size and turnover in Europe (2012).

Company category	Employees	Turnover	or	Balance sheet total
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

(Source: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm)

In addition, according to statistics of Finland the SMEs have less than 250 paid employees and their annual turnover is not more than 50 million euros and their balance sheet is not more than 43 million euros (Statistics Finland, 2003)

4.6 IPsec Authentication

The IPsec authentication proves legal user identity, protects data from outside attacks and provides data confidentiality. IPsec SAs (Security Associations) supports different types of authentication.

Pre-Shared secrets

Pre-shared secrets are a common password uses for identifying two or more peers. In Pre-shared secrets, the peer uses a public IP address to keep secret and identify another peer. Then both peers' starts sharing information's with each other, when an agreement point is reached between them they create necessary keys. The pre-shared secret is configured on both peers, so that they can identify another IP address and preliminary secret keys. The key generation process starts when primary identification is established. (Tiller, 2000)

PAP (Password Authentication Protocol)

PAP is point-to-point authentication protocol to validate users. It uses two way handshake such as password and username for authenticating a user. PAP provides all data as clear text. It cannot provide any protection against playback attack.

CHAP (Challenge Handshake Authentication Protocol)

The CHAP protocol is used to identify a remote user by using the three-way handshake system. It uses a layered authentication process to identify which is difficult to break. ISP (Internet Service Provider) provides PPP (Point-to-Point) session for users. When users dial a phone number, the ISP allows the user modem to establish PPP with a modem provided by ISP. Then, the CHAP session is ready to request a remote user's username and password. CHAP saves the user from playback attack by changing packet identifier, and a variable challenge value. The drawback of CHAP is that, it saves the secret key as clear text in the database. (Tiller, 2000)

4.7 IPsec in Action

IPsec is one of the strongest and ideal protocol for securing IP datagrams. It can protect any kind of traffic that passes on the IP packet. The IPsec mode applications detect IP traffic. The IPsec transport mode provides end-to-end security and the tunnel mode to prevent IP traffic. In addition, planning network security policies and their practical use reduce network traffic and keeps the data confidential.

4.7.1 End-to-end Security

By using the end-to-end security system, every IP packet is secured when they enter or leave a host. The security depends on user's policy selectors. SAs (Security Associations) are responsible for securing traffic between two user's endpoints. End-to-end security can be accomplished by using IPsec transport or tunnel mode but in tunnel mode, an extra IP header needs to be added.

Despite its advantages, end-to-end security has some drawbacks, too. The system uses different types of applications that need to inspect or modify and the transient packet will drop when end-to-end connectivity is established. Different quality of services like, fire walling, traffic shaping, traffic monitoring will remain unknown about the IP packet, so they are unable to make any decisions. NAT (Network Address Translation) does not work while running end-to-end network security.

The following figure is an example of end-to-end network security connection between two network hosts by using the IPsec VPN tunnel.

(Doraswamy & Harkins, 1999)

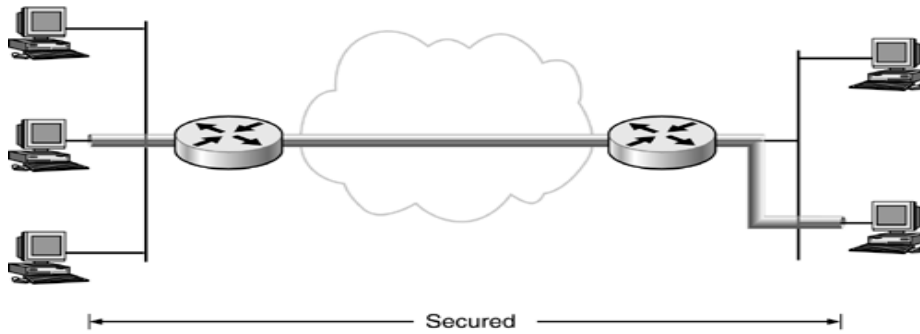


Figure 18. An end-to-end network security connected through the network. (Doraswamy & Harkins, 1999)

4.7.2 Network Security Policies and Implementation

A strong network security policy document should be written by a responsible management team and there should be a security goal. The security implementation is created based on security policies. This is the system to use and enforce the security policy.

“A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.” (Fraser et al., 1997)

In the following figure, the network security policy and implementation processes are explained. It is an excellent model for network admin and management teams to decide network security policies. The network security policies create data confidentiality, integrity and availability. Those policies can identify what needs to be protected and it can determine the type of threats. In addition, the security policies need to be reviewed and analyzed continuously and have to be improved each time when a weakness is found. However, the existing network security policies can be implemented in different ways, for example, through firewall, NAT, proxy, VPN and password encryption.

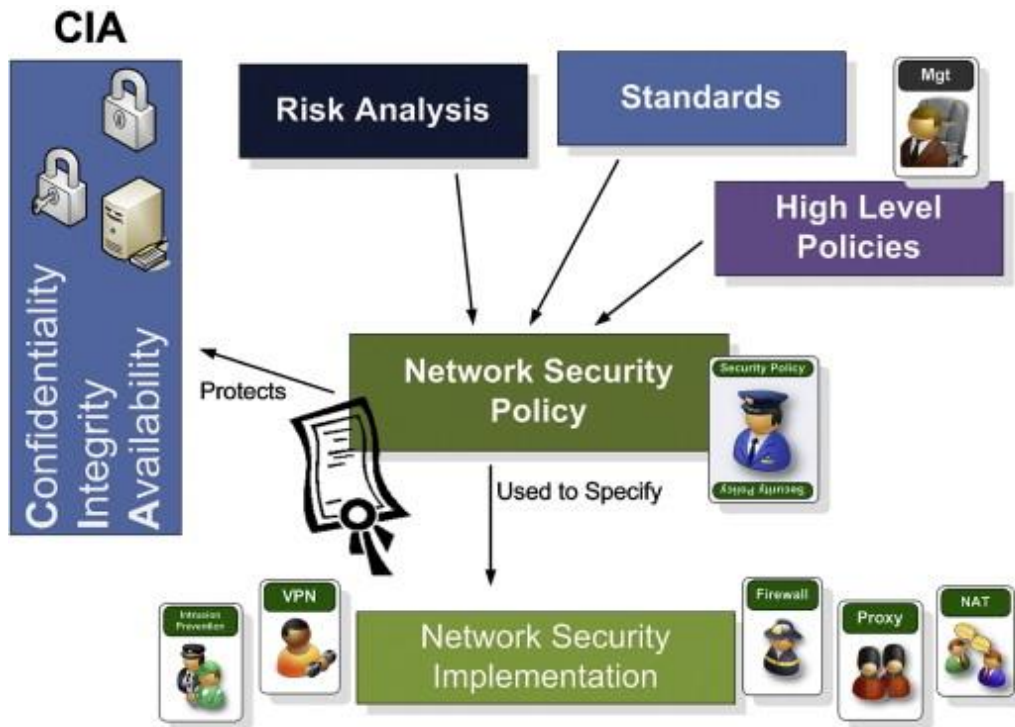


Figure 19. An example of network security policy and implementation system.
 (Source: <http://www.sciencedirect.com/science/article/pii/S0167404811001192#bib35>)

4.8 Configuring site-to-site IPsec VPN on Cisco Router

In this part, the site-to-site IPsec VPN tunnel has been established between two Cisco routers. The users must have to end-to-end IP connectivity before starting the configuration.

Components used: Cisco Router, model: 1841 and Cisco CP (Configuration Professional) version 2.5.

Note: The information used in this document taken from the Cisco website.

In the following diagram, a secure IPsec tunnel operating between Router A and Router B. The IP packet sending through the tunnel are secured by IPsec VPN. Here, several configurations are made on both routers to create a site-to-site IPsec VPN. These crucial configurations are:

1. Configuring ISAKMP (part-1)
2. Configuring IPsec (ISAKMP part-2, ACL (Access Control Lists) and Crypto Map.

The IPsec configurations on router B are described here:

Configuring ISAKMP policy and pre-shared keys:

```
Router-B (Configure) # crypto isakmp policy 2,
```

```
Authentication pre-share,
```

```
Crypto isakmp key cisco123 address 172.16.1.1.
```

Enable crypto transform configuration mode and crypto map SDM_CMAP_1:

```
R-B (con) # crypto ipsec transform-set Router-IPSEC esp-des esp-sha-hmac,
```

```
Description Tunnel to 172.16.1.1.
```

Set the IP address of remote end, match address and transform set:

```
R-B (con) #set peer 172.16.1.1,
```

Set transform-set Router-IPSEC,

Match address 100.

Configure FastEthernet0 interface to use crypto map SDM_CAMP_1:

R-B (con) #int fa0/0

Crypto map SDM_CAMP_1

Configuring access-lists and mapping with crypto map:

R-B (con) #access-list 100 remark SDM_ACL Category=4

Access-list 100 remark IPsec Rule

Access-list 100 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255

Configuring ACL 110 to identify traffic flows:

R-B (con) #access-list 110 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255,

Access-list 110 permit ip 10.20.10.0 0.0.0.255 any,

Route-map nonat permit 10,

Match ip address 110.

The configurations are identical on Router-A except access-lists and peer IP.

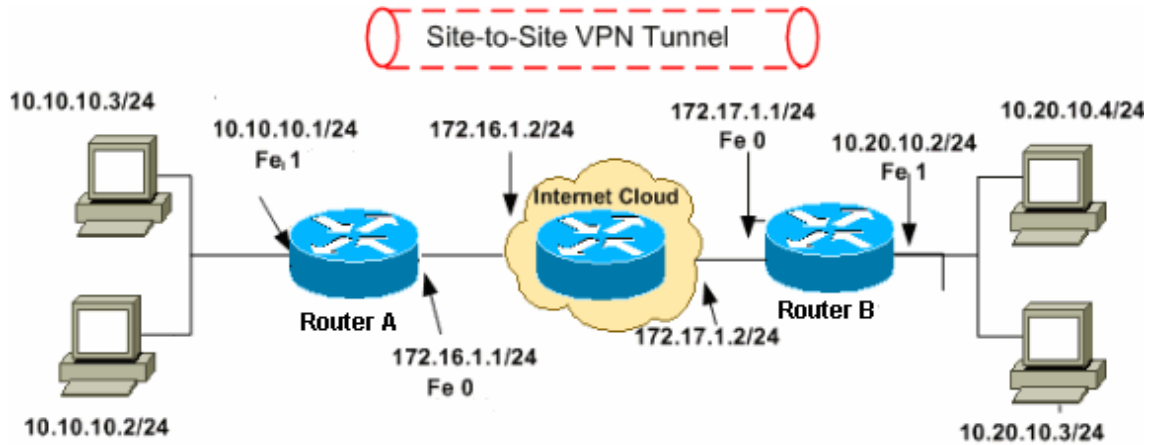


Figure 20. A site-to-site IPsec VPN are created between two Cisco routers.

(Source:<http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/113337-ccp-vpn-routerA-routerB-config-00.html#CCP2>)

5 CONCLUSION

The thesis is an explanation and a discussion of the VPN and IPsec protocol. It includes the process of the IPsec implementation system. The purpose of this thesis was to demonstrate the VPN service and to consider the IPsec VPN protocol for securing an SME's connection in remote areas. Sharing information or connecting branch offices from one place to other places over a public network is always a risk of injecting, altering or modifying the original data. Enterprise networks are the most common targets for hackers in order to abuse the information or to acquire the financial information.

To mitigate the enterprise network threats and vulnerabilities, the VPN is a reliable technology to create the private connection at low cost. In general, an enterprise uses the WAN service, provided by ISP to connect to their branch office. On the other hand, the WAN cost is higher than VPN cost and there is a risk of security threats when the data transfers over a public network. Compared with the WAN system, the VPN is a cost affordable, secure, and dependable service.

In summary, the VPN uses several authentication systems and establishes a private tunnel over a public network. Only the authorized users are permitted inside the network, so unauthorized users are unaware of the network tunnel. IPsec VPN can be implemented on hosts and router gateways. Thus, IPsec VPN is a suitable solution for SMEs so that they can implement it without expert knowledge. It is easier to implement the IPsec at SMEs than a corporate network, because of the small number of employees and branches.

In the future, there is an opportunity to increase the VPN service for the SMEs, to create private network at a low cost. The SMEs may consider an IPsec VPN for strong security and data confidentiality.

REFERENCES

Atakan, O., Badri, Z., Cho B., Lee, H.J., Schmid, A., Murhammer, M.W. 1999. A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management. IBM Publications.

Buchanan, W., Ekonomou, E., Fan, L., Macfarlane, R., Uthmani, O. 2012. Formal security policy implementations in network firewalls. At:<http://www.sciencedirect.com/science/article/pii/S0167404811001192#bib35>
Date of retrieval: 05-07-2015.

Carmouche, J.H. 2006. IPsec Virtual Private Network Fundamentals. Publisher: Cisco Press.

Cisco. 2007. IPsec VPN WAN Design Overview. Cisco system, Inc. At:https://www.cisco.com/application/pdf/en/us/guest/netso/ns171/c649/ccmigration_09186a008074f22f.pdf Date of retrieval: 05-13-2015.

Cisco. 2011. Configuring site-to-site IPsec VPN on Cisco Router. Cisco system, Inc. At:<http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/113337-ccp-vpn-routerA-routerB-config-00.html#CCP2> Date of retrieval: 05-12-2015.

Crawford, S., Tyson, J. How VPNs work [VPN benefits (Reliability)]. At:<http://computer.howstuffworks.com/vpn2.htm> Date of retrieval: 03-04-2015

Crawford, S., Tyson, J. How VPNs work (site-to-site and remote access VPN). At:<http://computer.howstuffworks.com/vpn3.htm> Date of retrieval: 05-04- 2015.

Davis, J., Liu, D., Lucas, M., Miller, S., Singh, A. 2006. Firewall Policies and VPN Configurations. Syngress Publishing, Inc.

Debashis, G. 2012. Network and Application Security-Fundamentals and Practices. NH: Science Publishers.

Doraswamy, N., Harkins D. 1999. IPsec, the New Security Standard for the Internet, Intranets, and Virtual Private Networks. New Jersey: Prentice-Hall, Inc.

Erin, M., Scott, C., Wolfe, P. 1999. Virtual Private Networks, Second Edition. O'Reilly Publications.

European Commission. 2014. SMEs structure and Turnover. At:http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm Date of retrieval: 05-24-2015.

Kozierok, C.M. 2005. IPsec Architectures and Implementation Methods. At:http://www.tcpipguide.com/free/t_IPSecArchitecturesandImplementationMethods-2.htm#Figure_117 Date of retrieval: 05-14-2015.

Loshin, P. 2003. Internet Control Message Protocol. At:<http://www.sciencedirect.com/science/article/pii/B9781558607828500245> Date of retrieval: 05-09-2015.

Microsoft Technet. 2005. IPsec mode (Tunnel and Transport). At:[https://technet.microsoft.com/en-us/library/cc737154\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc737154(v=ws.10).aspx) Date of retrieval: 04-16-2015.

Tiller, J.S. 2000. Technical Guide to IPsec Virtual Private Networks. Auerbach Publications.

Wikipedia. 2015. IPsec (Diagram and Framework of AH). At:<http://en.wikipedia.org/wiki/IPsec> Date of retrieval: 05-18-2015.

APPENDICES

These appendices describing and configuring site-to-site IPsec VPN on Cisco routers (4.5). The following appendices taken from the Cisco Websites:

Appendix 1. Cisco CP Configuration on Router A.

Select Configure > Security > VPN > Site-to-Site VPN then click the radio button next to Create a Site-to-Site VPN. Click Launch the selected task.

Configure > Security > VPN > Site-to-Site VPN


VPN

Create Site to Site VPN | Edit Site to Site VPN

Cisco CP can guide you through Site to Site VPN configuration tasks. Select a task, then click 'Launch the selected task' button.

Use Case Scenario

Site-to-Site VPN



Create a Site to Site VPN.

Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

Create a secure GRE tunnel (GRE over IPsec).

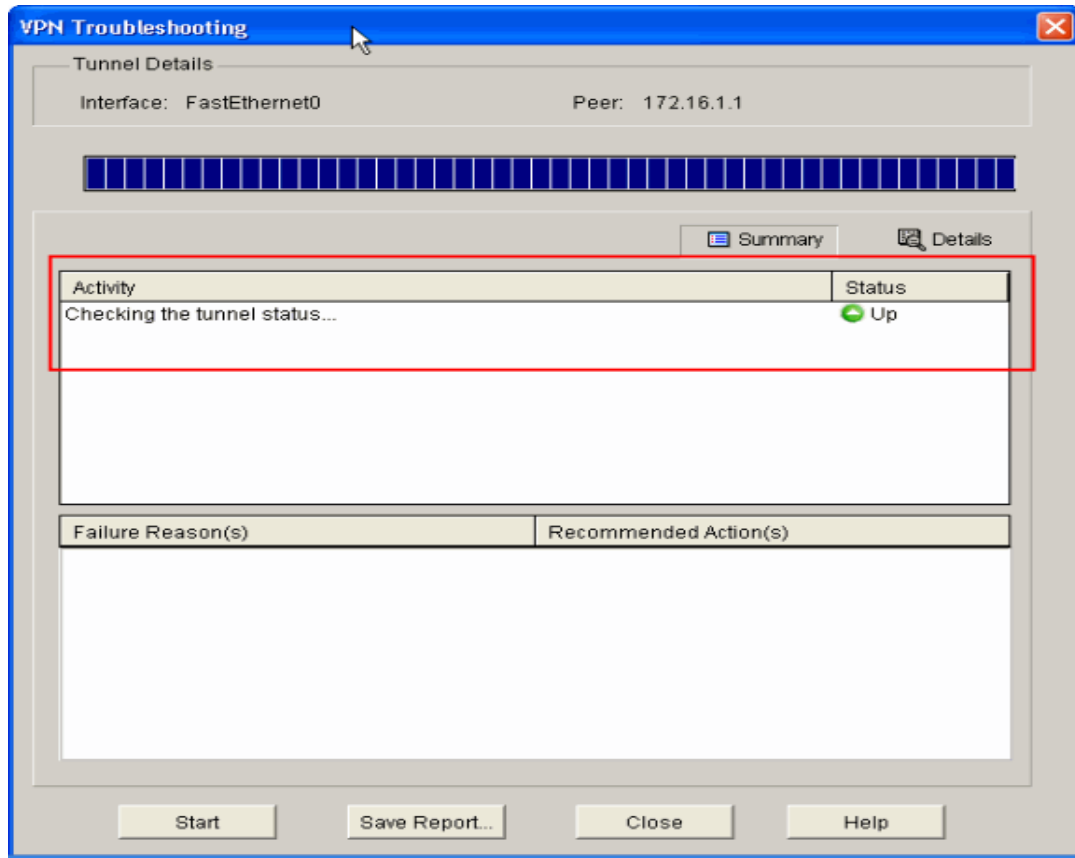
Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

Launch the selected task

The full Cisco CP Configuration on Router A and B are available at the Cisco website:

<http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/113337-ccp-vpn-routerA-routerB-config-00.html#CCP2>

The result of VPN connections.



Appendix 2. Router B CLI Configurations:

Building configuration...

!

!

Crypto isakmp policy 2

Authentication pre-share

!--- Specifies the pre-shared key "cisco123" which should

```
Crypto isakmp key cisco123 address 172.16.1.1
```

```
!--- Configuration for IPsec policies.
```

```
!--- Enables the crypto transform configuration mode,
```

```
Crypto ipsec transform-set Router-IPSEC esp-des esp-sha-hmac
```

```
!
```

```
!--- Indicates that IKE is used to establish
```

```
!--- the IPsec Security Association for protecting the
```

```
!--- traffic specified by this crypto map entry.
```

```
Crypto map SDM_CMAP_1 1 ipsec-isakmp
```

```
Description Tunnel to172.16.1.1
```

```
!--- Sets the IP address of the remote end.
```

```
Set peer 172.16.1.1
```

```
!--- Configure the access-lists and map them to the Crypto map  
configured.
```

```
Access-list 100 remark SDM_ACL Category=4
```

```
Access-list 100 remark IPsec Rule
```

```
Access-list 100 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

```
!--- This ACL 110 identifies the traffic flows using route map
```

```
Access-list 110 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

```
Access-list 110 permit ip 10.20.10.0 0.0.0.255 any
```

```
route-map nonat permit 10
```

```
  Match ip address 110
```

```
!
```

```
!
```

These are the key configurations of IPsec VPN on Router B. The full Configurations are available at the Cisco website:

<http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/113337-ccp-vpn-routerA-routerB-config-00.html#CCP2>

