Implementing Virtual Private Network using Ipsec Framework
With Cisco Packet Tracer

Wassan Saad Hayale
AL-Iraqia University
Administration and Economic College
Baghdad, Iraq

Elaf Ayyed Jebur
Baghdad University
College of Medicine; IT unit
Baghdad, Iraq

Abstract—Virtual Private Network used to create an end-
to-end tunnel over third-party networks such as the Internet
or extranets. It cannot guarantee that the information
remains secure while traversing the tunnel. There are many
different types of VPN technologies available such as Internet
Protocol Security, SSL, MPLS, L2F, PPTP, L2TP and GRE.
IPSec has become a much more popular VPN security. It
provides a framework for configuring secure VPN. This paper
shows how we can implement the Virtual private network
with Cisco provided tool Packet Tracer which is an
integrated simulation, visualization, collaboration, and
assessment environment for networking novices to design,
configure, and troubleshoot computer networks at a CCNA-
level of complexity.

Keywords—VPN; IPSec; Packet Tracer; Tunnel; CCNA.

I. INTRODUCTION

If we break down the term virtual private network into
its individual components, we could say that a network
allows connectivity between two devices. Those two
devices could be computers on the same local-area network
or could be connect over a wide area Network. In either
case, a network is providing the basic connectivity between
the two [1].

The word virtual in VPN refers to a logical connection
between the two devices. For example, one user may be
connected to the Internet in location, another user may be
connected to the Internet in Vienna, Austria, and we could
build a logical network, or virtual network, between the two
devices using the Internet as our Transport mechanism. The
letter P in VPN refers to private. The virtual network we
could create between our two users in Las Vegas and
Vienna would be private between those two parties.
Therefore, there are the basics for VPN, a virtual private
network [1].

Unfortunately, if we did have a VPN established
between two devices over the Internet, what would prevent
an individual who had access to the packets from
eavesdropping on the conversation? The answer is not
much, by default. Therefore, in addition to most VPNs, we
add the ingredients of confidentiality and data integrity so
that not anyone who is eavesdropping can make sense of the
data because it is encrypted and they do not have the keys
required to decrypt or unlock the data to see what the data
actually is. The confidentiality provided by the encryption
could also represent the P in VPNs. We also use integrity
checking to make sure that our VPN is correctly seeing the
packets as they were sent from the other side of the VPN
and that they are not being altered or manipulated
maliciously along the path [1].

Using the example of the user in Vienna and Las Vegas,
why would we ever want to use a VPN between the two?
We do have other options for connectivity. We could
purchase each user a dedicated WAN connection from
Vienna to Las Vegas. Each user could connect to his local
side and communicate with each other over the dedicated
link. One of the obvious problems with this is cost. It is
much cheaper to connect the user to the Internet through a
local service provider than to purchase a dedicated circuit
that goes to only one other destination [1].

II. TWO MAIN TYPES OF VPN

There are two major categories into which VPNs could
be placed: remote access and site-to-site. The following are
details about each, including when they might be used:

A. Remote-access VPNs:

Some users might need to build a VPN connection from
their individual computer to the corporate headquarters (or
to the destination, they want to connect to). This is referred

Virtual Private Network =Tunneling + Encryption

Fig 2. Traditional IPSEC VPN [2].
to as a remote-access VPN connection. Remote-access VPNs can use IPsec or SSL technologies for their VPN [1].

B. Site-to-site VPNs:

The other main VPN implementation is by companies that may have two or more sites that they want to connect securely together (likely using the Internet) so that each site can communicate with the other site or sites. This implementation is called a site-to-site VPN. Site-to-site VPNs traditionally use a collection of VPN technologies called IPsec [1].

III. MAIN BENEFIT OF VPN

The main benefits of using a VPN for either remote access or site to site, include the following:

a. Confidentiality:
Confidentiality: means that only the intended parties can understand the data that is sent. Any party that eavesdrops may see the actual packets, but the contents of the packet or the payload are scrambled (also called cipher text) and meaningless to anyone who cannot unlock or decrypt the data. The major goal of a VPN is confidentiality, and the sender encrypting the data or the packet that needs to be protected and then sending it over the VPN accomplishes it. The receiver of the packet or data then faces the same challenge as the eavesdropper, in that the data must be decrypted to make sense out of it. The algorithms and formulas for encrypting data are publicly available and are well known. The part that makes the message secret is the key or “secret” that is used to encrypt the data. If the sender and the receiver both know, the key that is used, they can encrypt and decrypt information back and forth using the same key or keys, and anyone in the middle who does not know the key or keys that were used cannot decrypt [1].

b. Data Integrity

If two devices are communicating over a VPN, another important factor about the data that is being sent is to make sure it is accurate from end to end. If an attacker injects bits or data into the packets of a VPN session, data integrity could suffer if the modification of the data goes undetected [1].

c. Authentication

A VPN tunnel is fantastic in that you can encrypt data and verify that data has not been modified while in transit. But what if you have established, a VPN tunnel, directly to the attacker’s computer? Being able to validate or authenticate the device that you are connected to is an important aspect of a good VPN. You can authenticate the peer at the other end of the VPN tunnel in several different ways, including the following [1]:

- Pre-shared keys used for authentication only
- Public and private key pairs used for authentication only
- User authentication (in combination with remote-access VPNs) [1]

d. Anti-replay

If an attacker watches your VPN traffic and captures it with the intent to replay it back and fool one of the VPN peers into believing that the peer trying to connect is a legitimate peer, an attacker might be able to build a VPN pretending to be a different device. To solve that, most implementations of VPNs have an anti-replay functionality built in. This just means that once a VPN packet has been sent and accounted for, that exact same VPN packet is not valid the second time in the VPN session [1].

IV. INTERNET PROTOCOL SECURITY-IPSEC:

A “framework” of open standards developed by the IETF to create a secure tunnel at the network (IP) layer.

- It spells out the rules for secure communications.
- RFC 2401 - RFC 2412 [2].

IPsec is not bound to any specific encryption or authentication algorithms, keying technology, or security algorithms [3]. IPsec allows newer and better algorithms to be implemented without patching the existing IPsec standards [3].
5. THE GOAL METHOD THAT PROVIDES THE FEATURE BY IPSEC

1) Confidentiality: Provided through encryption changing clear text into cipher text. Achieved through encryption of traffic as it travels down the VPN. The shorter the key, the easier it is to break. Represented by DES, DES3, AES, and SEAL [2].

2) Integrity: Provided through hashing and or through Hashed Message Authentication Code (HMAC) to verify that data has not been manipulated during its transit across the network. Achieved by MD5, SHA, HMAC-MD5, HMAC-SHA [1].

3) Authentication: Provided through authenticating the VPN peers near the beginning of a VPN session. The device on the other end of the VPN tunnel must first be authenticated using:
   a. PSK. A pre-shared secret key value is entered into each peer manually.
   b. RSA. The exchange of digital certificates authenticates the peers [1].

4) Anti-replay support: When VPNs are established, the peers can sequentially number the packets, and if a packet is attempted to be replayed again (perhaps by an attacker), the packet will not be accepted because the VPN device believes it has already processed that packet. So the DES, 3DES, HMAC… require a
symmetric, shared key for encryption and decryption. Diffie-Hellman key agreement is a public key exchange method that provides a way for two peers to establish a shared secret key. Variations of the DH key exchange are specified as DH groups [1].

a. DH groups 1, 2, and 5: key size of 768, 1024, 536 bits.

b. DH groups 14, 15, and 16: key sizes with 2048, 3072, 4096 bits.

c. DH groups 19, 20, and 24: key sizes 256, 384, 2048 bits [1].

VPN peers negotiate which DH group to use. When VPNs are established, the peers can sequentially number the packets, and if a packet is attempted to be replayed again (perhaps by an attacker), the packet will not be accepted because the VPN device believes it has already processed that packet [1].

VI. IPSEC FRAMEWORK PROTOCOLS.

IPsec uses two main protocols to create a security framework:

1. AH (Authentication Header):

   a) IP protocol 51.

   b) Used when confidentiality is not required.

   c) Provides data authentication and integrity.

   d) Integrity does not include changeable fields as TTL [5].

The IP header and data payload are hashed using the shared secret key. The hash builds a new AH header, which is inserted into the original packet [5].

2. ESP (Encapsulating Security Payload)

   a) IP protocol 50

   b) Can provide confidentiality, integrity, and authentication [5].

The ESP Trailer & ESP header are added to the packet. Then the payload with the ESP Trailer are encrypted. Then the encrypted payload and the ESP header is sent through a hash algorithm [2].
When both authentication and encryption are selected, encryption is performed first. ESP Authentication includes the ICS (Integrity Check Value).

VII. IPSec MODES:

A. Transport Mode.

Security is provided only for the Transport Layer of the OSI model and above. The original IP address is used to route the packet through the Internet. Works well with GRE [5].

B. Tunnel Mode.

Provides security for the complete original IP packet. The original packet is encrypted and encapsulated in another packet (IP-in-IP encryption) [5].

Used in the IPSec remote-access application where a home office might not have a router to perform the IPSec encapsulation and encryption [5].

Peers negotiate key exchange parameters, establishes a shared key, authenticates the peer, and negotiates the encryption parameters [5].

SA (Security Association) is the negotiated parameters between two devices. Maintained within a SADB (SA database), which is established by each device [5].

VIII. CRYPTOSYSTEM

A system to accomplish the encryption/decryption, user authentication, hashing, and key-exchange processes. A cryptosystem may use one of several different methods, depending on the policy intended for various user traffic situations [2].

IX. CONFIGURING IPSec VPNs

A. Site-to-Site VPN

Step 1 – Configure Interesting Traffic

We need first to define the Interesting Traffic, that is, traffic that we want to encrypt. Using Access-Lists (Crypto ACL). Configure ACL 100 to identify the traffic from the LAN on R1 to the LAN on R2 as interesting. In our configuration diagram above, we want all traffic flow between private networks 192.168.10.0/24 and 172.16.20.0/24 to be encrypted. However, not all other traffic from LAN-1 or LAN-2 to the Internet will pass through the VPN tunnel.

Step 2 – Create ISAKMP (IKE) policy (phase 1)

a. The transform sets, hash methods, and other parameters are determined. The initiator sends proposals to another router the responder takes. The proposal defines which encryption and authentication protocols are acceptable. The protocols are grouped into sets, called IKE policy sets. If a policy match is found between the peers, IKE Phase 1 continues. Policy set numbers are only locally significant to a VPN device.

b. The second exchange creates and exchanges the DH public keys. All further negotiations are encrypted using the DH-generated secret key.

c. Then peers authenticate each other using PSK or RSA signature or RSA encrypted nonce. This PSK must be identical on both peers.
Step 3 – Configure IPsec transform set (phase 2)

The goal of Phase 2 is to establish a secure IPSEC session between peers. We negotiation of IPSEC security parameters and IPSEC transform set. It represents an IPsec security protocol (AH or ESP) plus the associated algorithm. Multiple transform set can be configured. During the negotiation, the peers search for a transform set that has the same criteria. When found, it is applied to the protected traffic as part of the IPsec SAs of both peers. Therefore we create the transform-set VPN-SET to use esp-3des and esp-sha-hmac. To define a transform set

```
crypto ipsec transform-set ttl esp-3des esp-sha-hmac
```

![Image: Fig 19. Configuring IPSEC phase 2.]

Step 4 – Create a crypto ACL

In this step, we create the crypto map xx that combines the needed configuration parameters of IPsec SAs. Only one crypto map can be set to a single interface. If more than one crypto map entry is created for a given interface, use the sequence number.

```
crypto map xx 10 ipsec-isakmp
set peer 200.1.1.2
set transform-set ttl match address 100
```

Step 5 – Create and apply the crypto map.

Apply the crypto map to the outgoing interface of the vpn tunnel. Then ensure that the routing information needed to send packets into the tunnel is configured.

```
interface Serial1/0
ip address 200.1.1.1 255.255.255.252
clock rate 128000
crypto map xx
```

![Image: Fig20. Applying the crypto maps.]

Fig 21. Five steps of IPSEC configuration.

![Image: Fig 22. Site to site topology using packet tracer.]

B. Remote Access VPN

i. Put a host name to router, Put an IP to the two interfaces.
ii. Configure the Authentication for remote user.

There are a couple of different ways to authenticate and authorize remote users in order to access network resources via the VPN. The “Authentication, Authorization, and Accounting” mechanism (AAA) of the router is used for such a task. The simplest way is to use Local usernames/passwords configured on the Router for authentication and authorization.

Remote users must be “authenticated” first to login to the VPN tunnel, and then must be “authorized” to use the network resources. Therefore, we must configure the router device for both “login authentication” and “network authorization”.

iii. Create username and password

```
R1(config)#username admin password cisco
```

iv. Create pool of IPs to remote user

Configure an IP address pool that will be used to assign IP addresses to remote users

```
R1(config)#ip local pool x1 192.168.1.100 192.168.1.120
```

v. Create apolicy between two routers

```
R1(config-isakmp)#crypto isakmp policy 10
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 1
R1(config-isakmp)#lifet ime-time 86400
```

vi. Create a policy and parameters that a specific group give to the client

```
R1(config)#crypto isakmp client config group q
R1(config-isakmp-group)#key cisco
R1(config-isakmp-group)#pool x1
R1(config-isakmp-group)#exit
```

vii. Encrypt key to encrypt payload

```
R1(config)#crypto isakmp transform-set transform esp-3des esp-md5-hmac
```

viii. Create a dynamic map for remote client profile

```
R1(config)#crypto dynamic-map x1 10
R1(config-crypto-map)#sec transform-set transform esp-3des esp-md5-hmac
R1(config-crypto-map)#reverse-route
R1(config-crypto-map)#exit
```

ix. Create static map, define which client use dynamic map

```
R1(config)#crypto map x5 client authentication list test
R1(config)#crypto map x5 isakmp authorization list test
R1(config)#crypto map x5 client configuration address respond
R1(config)#crypto map x5 10 isakmp dynamic x2
```

Attempts to change dynamic map tag for existing crypto map is ignored.

x. Apply static map on specific interface

```
R1(config)#int Fa0/0
R1(config-if)#crypto map x3
```

These steps have similarities with site-to-site VPN configuration where we had one site with a dynamic IP address. Since the IP address of the remote VPN users will be unknown (dynamic) to the central site router, we have to create a dynamic crypto map.

```
R1(config)#crypto isakmp transform-set transform esp-3des esp-md5-hmac
```

```
R1(config)#crypto dynamic-map x1 10
R1(config-crypto-map)#sec transform-set transform esp-3des esp-md5-hmac
R1(config-crypto-map)#reverse-route
R1(config-crypto-map)#exit
```

x. Apply static map on specific interface

```
R1(config)#int Fa0/0
R1(config-if)#crypto map x3
```

```
R1(config)#crypto isakmp transform-set transform esp-3des esp-md5-hmac
```

```
R1(config)#crypto dynamic-map x1 10
R1(config-crypto-map)#sec transform-set transform esp-3des esp-md5-hmac
R1(config-crypto-map)#reverse-route
R1(config-crypto-map)#exit
```

X. CONCLUSIONS

Nowadays the use of the Internet has become very common in telecommunications and data transfer tasks. So it became important to secure data transfer since current Internet protocols do not protect data sufficiently enough. Firewall programs may provide protection to the information coming into the network, but what about the information that traveling the network. If leased lines are used, it is very expensive, especially at long distances between enterprise networks. Therefore, it became necessary to use the technique that provide the security and in the same time not expensive. Therefore, the VPN technique have been used and a set of standard security Internet Protocols known as IP Security (IPSec) have been developed. With the use of this technique, it has become possible to provide reliability and data integrity. Since we relied on the Internet, which could be very attractive in terms of low cost VPN unlike leased lines. It helps to make the possibility of business to expand their services over a long distance. Enterprise that deploy site-to-site IPSec VPN have a complete control on their WAN routing. The major advantage of this technique that it is invisible. The user dose not worry about the security of the data transfer and even though he will not notice that. Moreover, the IPSec protocol is the only protocol that secure all the traffic since it relay in network layer. Also it is not application specific,
that’s mean it can protect any application since this protocol is compatible with many other protocol and it work with equipment from many different manufactures but in the same time the technologies from different creators may work poorly together. Also one of the positive features of IPSec that it is possible to change the algorithm for encryption, authentication, and hashing. Therefore, we can replay one algorithm with another more secure. However, this can be a disadvantage as well since some default algorithm considered cracked such as MD5 hash algorithm and DES encryption algorithm. Unfortunately, like any other technologies it must come with some drawback. One of these drawbacks is it should not support multiprotocol and IP multicast traffic. In addition, it imposes a CPU overhead due to the procession needed for encryption, decryption, and authentication. It is difficult to scale due to that the IPSec tunnel need a provision between each peers. In addition, deployment requires a high level of knowledge and understand of security factors. Moreover, the performance are difficult to control like the speed of data transfer as it is lower than traditional connectivity. In addition, having many VPN connection at the same time can considerably slow down the network. Also using a computer not provided by your company to connect to VPN may possess security risk. In addition, it relies on your pubic key. Therefore, if you have poor key management then you will loss the security factor. Despite the pros and cons of virtual private networks, they still offer a viable solution for secure communications between distributed users and many people find the significant benefits of these networks worth the effort of dealing with their potential difficulties.

REFERENCES