Implementation of Site-To-Site IPSEC Virtual Private Network For Enterprise Network Design Using Cisco Packet Tracer Simulation Tool

Dr Rajamohan Parthasarathy[1] School of IT SEGi UniversityMalaysia.

Mr Seow SoonLoong[2]
School of IT SEGi University Malaysia
Ms Preethy Ayyappan[3] Faculty of EBE SEGi UniversityMalaysia.
Ms Zainab AbdulHamid[4]
School of IT SEGi UniversityMalaysia.
Mr A. SenthilKumar[5]
Dept of Comp. Sci.PRIST(Deemed University) Madurai Campus.

Abstract — A Virtual Private Network (VPN) is a network that is constructed using public wires usually the Internet to connect remote users or regional offices to a company's private, internal network. A VPN works byusing the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. 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 (IPSec), SSL, MPLS, L2F, PPTP, L2TP and GRE. IPSec has become a much more popular VPN security. It provides a framework for configuring secure VPN. A VPN protects the private network, using encryption and other security mechanisms to confirm that only authorized users can access the system and the data can be intercepted. As the IPSec protocol is able to provide the highest level of security, using IPSec VPN to build security Intranet has become a trend. This paper explore how we can implement the Site-to-Site IPSec Virtual private network for enterprise network design using with Cisco provided tool Packet Tracer which is an integrated simulation, visualization, collaboration, and assessment environment for networking novices to design, configure, andtroubleshooting operations and maintenance.

Keywords — *Virtual Private Network (VPN), Internet Protocol Security (IPSec), Internet Key Exchange (IKE), Internet Security Association and Key Management Protocol (ISAKMP), Advanced Encryption Standard (AES), Data Encryption Standard (DES), Message Digest 5 (MD5).*

I. INTRODUCTION

Internet, as a communication platform, is a basic communication system today. A **Virtual Private Network** (**VPN**) extends a private network across a public network, such as the Internet. Virtual Private Networks (VPN) can be used to establish a high level of security in network communication. Virtual means that the connection is dynamic. It can change and adapt to different circumstances using the internet's fault tolerant capabilities. When a connection is required it is established and maintained regardless of the network infrastructure between endpoints. When it is no longer required the connection is terminated, reducing costs and the amount of redundant infrastructure. Private means that the transmitted data is always kept confidential and can onlybe accessed by authorised users. This is important because the internet's original protocols TCP/IP (transmission control protocol/internet protocol) were not designed to provide such levels of privacy. Network is the entire infrastructure between the endpoints of users, sites or nodes that carries the data. It is created using the private, public, wired, wireless, internet or any other appropriate network resource available. (Tripti Sharma et al., 2015).

VPN technology enables high-security networking using distributed or public network infrastructure. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions. Major implementations of VPNs include OpenVPN and IPsec. VPN technology transmits potentially “sensitive” information, which can be classified as secret or confidential through insecure networks. VPN system is based on setting up of so-called “communication tunnels”, previously secured using various cryptographic methods (algorithms). It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

Types of VPN There are 2 common types of virtual private network, which are remote access VPN and site-to-site VPN.

1. Remote Access VPN

Remote access VPN is very common VPN service that you can set up in your office or home network. It can be implemented by setting up a VPN gateway or server and you can connect to it by using VPN client from other locations. If not, you can also subscribe to VPN service provided by a VPN provider for similar secure access too. The remote access VPNis supported by L2F, PPTP, L2TP and IPsec tunneling protocols. Sometimes if the user uses the web browser instead of VPN client to connect to VPN gateway, we call this type of VPN as SSL VPN.

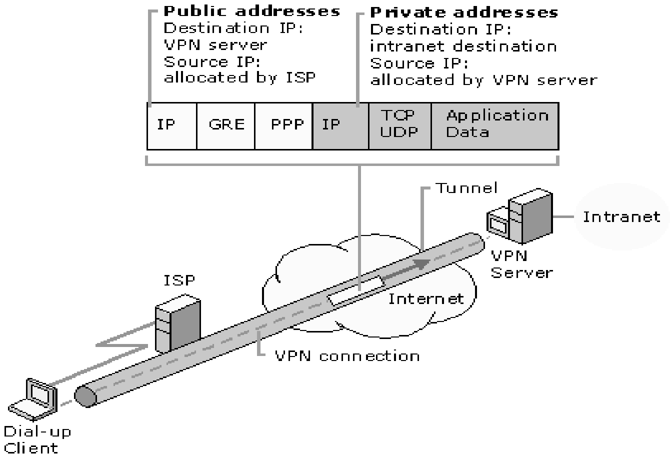


Fig. 1. Overview of functioning of a Remote Access VPN Network

2. Site-to-Site VPN: Site-to-site VPN is the VPN connection established between 2 VPN gateways that reside in 2 different networks over the Internet, so that both networks' computers can exchange data securely. There is no VPN client needed on user computers. The VPN connection will be established between both VPN gateways. Both VPN gateways will encrypt and decrypt the communication data to ensure the security and integrity of data (Mohd Nazri Ismail et al., 2009). The site-to-site VPN can be supported by IPsec tunnel mode, PPTP, L2TP over IPsec tunneling protocols.

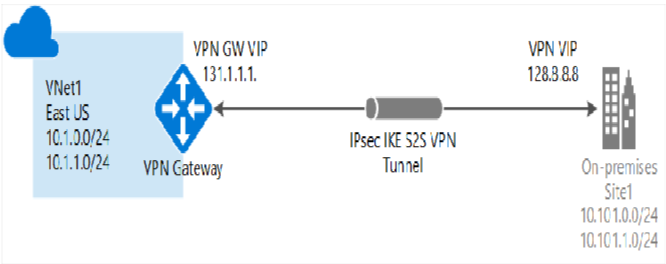


Fig. 2. Site-to-Site VPN Gateway cross-premises connectiondiagram, Source: Docs.microsoft.com

II. TECHNICAL REVIEW ON VPN SECURITYVirtual Private Network

In this paper we studied how VPN maintains privacy of data through security procedures and tunneling protocols. In effect, data is encrypted at sender's side and forwarded via "tunnel" which is then decrypted at receiver's side. **There are three primary components:**

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Internet Key Exchange (IKE) protocols.

2.1 Authentication Header (AH)

The IP Authentication Header (AH) is used to provide

- Connectionless integrity
- Data origin authentication for IP data grams.
- Anti-replay protection, which protects againstunauthorized retransmission of packets.

AH can be used in two modes.

- **Tunnel mode**- AH creates new IP header for eachpacket.
- **Transport mode**- no new header is created.

Integrity and authentication are provided by the placement of the AH header between the IP header and the transport (layer 4) protocol header, which is shown as: AH may be applied alone or in combination with the IP Encapsulating Security Payload (ESP). ESP when used with AH provides same anti-replay and integrity services with add on service of data confidentiality.

2.2 Encapsulating Security Payload (ESP)

ESP is the second core security protocol which provides authentication, integrity, and confidentiality which protects against data tampering and most importantly, provides message content protection. ESP also provides all encryption services. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content froman unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data Like AH, ESP can also be used in two modes: transport and tunnel. In tunnel mode, ESP creates a new IP header for each packet. This mode encrypts and protects the integrity of both IP header and data. While in transport mode no new IP header is created so ESP can only encrypt and protect the integrity of the data (Tripti Sharma et al., 2015)

2.3 Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is the protocol used to set up a security association (SA) in the IPsec protocol suite and to exchange keys between parties transferring data. Before secured data can be exchanged, a security agreement between the two computers must be established **(**William Stallings, 2013). In this security agreement, called as security association (SA), both agree on how to exchange and protect information.

2.4 IPsec VPN Working

When IPsec VPN is used, a virtual "tunnel" connecting the two endpoints is created. Configure which packets aresensitive. Once configured, an IPsec peer sends the packet through the tunnel to the remote peer. The traffic within the VPN tunnel is encrypted so that other users of the publicInternet can not readily view intercepted communications (Andrew Mason, 2002).

2.5 SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's Computer. It is used to give remote users with access to Web Applications, client/server applications and internal network connections.

2.6 SSL VPN Working

An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor. (R. Deal, 2005).

2.7 Cryptography

In Cryptography parlance, A's message is called "**Plaintext**" .The process of scrambling the message is referred to as **"Encryption".** After encryption of the message, the scrambled version is called "**Cipher Text**. "From the Cipher text, and can recover the original unscrambled messagevia "**Decryption".** (Rosenberg, 2002).

III. METHODOLOGY OF VPN IPSEC SOLUTIONS

IPsec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network (VPN). IPsec Tunnel mode is used to secure gateway-to-gateway traffic. IPsec Tunnel mode protects the entire contents of the tunneled packets. The IPsec (George Dragoi, 2012) Tunnel mode data packets sent from the source device are accepted by the security gateway (a router or a server) and forwarded to the other end of the tunnel, where the original packets are extracted and then forwarded to their final destination device IPsec tunnel is usually built to connect two or more remote LANs via Internet so that hosts in different remote LANs are able to communicate with each other as if they are all in the same LAN.

Methods of managing VPN IPsec Tunneling Technology inenhancing security level

1. Highlight the role of VPNs in enhancing communications security for all sizes of businesses, especially the large enterprise networks with Cisco Router and Security Device Manager (SDM).

2. Illustrate the role of IPsec tunneling technology in VPN connection between two LANs (site-to-site VPN) or a remote dial-up user and a LAN.

3. Study the role of Cisco Easy VPN server in facilitating the deployment process of virtual private network (VPN) for remote offices.

4. IPsec Tunneling Technology

A secure network must begin with robust security policies that dictate the security deployment in the network, and IPsec protocol is one of examples for securing the transfer process of information at the OSI layer. The job of IPsec suite takes placed at the Network Layer, for protecting and authenticating aim of IP packets between sharable IPsec peers. So, the function of this protocol relies on protecting all application traffic virtually, due to the protection ability to be implemented from Layer 4 through Layer 7 (Yang, 2011).

For providing the framework and the network administrator in IPsec, there is just a need to select the appropriate algorithms for being sure that the similar algorithms are used between two parts, and for investigating the security services. Without obligation of IPsec to particular algorithms, novel and better algorithms will be allowed to be performed in the IPsec frame. It has the ability to secure the track between site-to-site gateways, the couple of hosts, or to secure a track between gateway and host, which implemented the remote access. (Muirhead & Page, 2010).

A VPN connection connects two LANs (site-to-site VPN) or a remote dial-up user and a LAN. Flowing traffic between connected points passes out of shared resources. So, IPsec tunnel is used for securing VPN communication at passing time. IPsec tunneling technology protects entire IP packets, byencrypting the original packets after wrapping it, then it sends new IP header after adding it to the other side of the VPN tunnel (IPsec peer) (Muirhead & Page, 2010).

Weprovide an example of IPsec tunneling mode between a connected Cisco VPN Client and an IPsec Gateway. First, the traffic from the client is encrypted, and then encapsulated in a novel IP packet, after that it sent to the other end. When the traffic is decrypted by the firewall, the original IP packet ofthe client is sent to the local network (Snader, 2015). AH or ESP header of IPsec is inserted between both header of the IP and the upper layer protocol. ESP is used more that AH in Tunneling configuration of IPsec-VPN.

IV. VPN SITE-TO-SITE IPSEC IMPLEMENTATION &TESTING

Scenario

The network topology shown three routers and the task is to configure R1 and R3 to support a site-to-site IPsec VPN when traffic flows between their respective LANs. The IPsec VPN tunnel is from R1 to R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN.

IPsec provides secure transmission of sensitive information over unprotected networks, such as the Internet. IPsec operates at the network layer and protects and authenticates IP packets between participating IPsec devices (peers), such as Cisco routers.

Part 1: Configure IPsec Parameters on R1Part 2: Configure IPsec Parameters on R3Part 3: Verify the IPsec VPN

Table 1. IP **Addressing Table for the Scenario**

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Table 2. ISAKMP Phase 1 Policy Parameters

Parameters		R1	R3
Key Distribution Method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption Algorithm	DES, 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication Method	Pre-shared keys or RSA	pre-share	pre-share
Key Exchange	DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		vpnpa55	vpnpa55

Table 3. IPsec Phase 2 Policy Parameters

Part 1: Configure IPsec Parameters on R1 **Step 1: Test connectivity.**

Ping from PC-A to PC-C.

Step 2: Enable the Security Technology package.

a. On R1, issue the **show version** command to view theSecurity Technology package license information.
b. If the Security Technology package has not been enabled,use the following command to enable the package.
c. Accept the end-user license agreement.
d. Save the running-config and reload the router to enable thesecurity license.
e. Verify that the Security Technology package has beenenabled by using the **show version**command.

Step 3: Identify interesting traffic on R1.

Configure ACL 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting trafficwill trigger the IPsec VPN to be implemented when there is traffic between the R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Because of the implicit **deny all**, there is no need to configure a **deny ip any any** statement.

Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.

Configure the **crypto ISAKMP policy 10** properties on R1 along with the shared crypto key **vpnpa55**. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured. Therefore, only the encryption method, key exchange method, and DH method must be configured. **Note**: The highest DH group currently supported by Packet Tracer is group 5. In a production network, you would configure at least DH 14.

Step 5: Configure the IKE Phase 2 IPsec policy on R1.

a. Create the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac.**
b. Create the crypto map VPN-MAP that binds all of the Phase2 parameters together. Use sequence number 10 and identify itas an ipsec-isakmp map.
Step 6: Configure the crypto map on the outgoinginterface.
Bind the VPN-MAP crypto map to the outgoing Serial 0/0/0interface.

Parameters	R1	R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Part 2: Configure IPsec Parameters on R3

Step 1: Enable the Security Technology package.
a. On R3, issue the show version command to verify that the Security Technology package license information has been enabled.
b. If the Security Technology package has not been enabled, enable the package and reload R3.
Step 2: Configure router R3 to support a site-to-site VPNwith R1: Configure reciprocating parameters on R3.
Configure ACL 110 identifying the traffic from the LAN onR3 to the LAN on R1 as interesting.

Step 3: Configure the IKE Phase 1 ISAKMP properties onR3: Configure the crypto ISAKMP policy 10 properties on R3 along with the shared crypto key vpnpa55.

Step 4: Configure the IKE Phase 2 IPsec policy on R3:
a. Create the transform-set VPN-SET to use **esp-aes** and **esp- sha-hmac**.
b. Create the crypto map VPN-MAP that binds all of the Phase2 parameters together. Use sequence number 10 and identify itas an ipsec-isakmp map.

Step 5: Configure the crypto map on the outgoing interface: Bind the VPN-MAP crypto map to the outgoingSerial 0/0/1 interface.

Part 3: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.
Issue the **show crypto ipsec sa** command on R1.

Note that the number of packets encapsulated, encrypted,decapsulated & decrypted are all set to 0.
Step 2: Create interesting traffic.
Ping PC-C from PC-A.
Step 3: Verify the tunnel after interesting traffic. On R1, re-issue the **show crypto ipsec sa** command.**Step 4: Create uninteresting traffic.**
Ping PC-B from PC-A. **Note**: Issuing a ping from router R1 toPC-C or R3 to PC-A is not interesting traffic.
Step 5: Verify the tunnel.
On R1, re-issue the **show crypto ipsec sa** command.

Solution - Topology

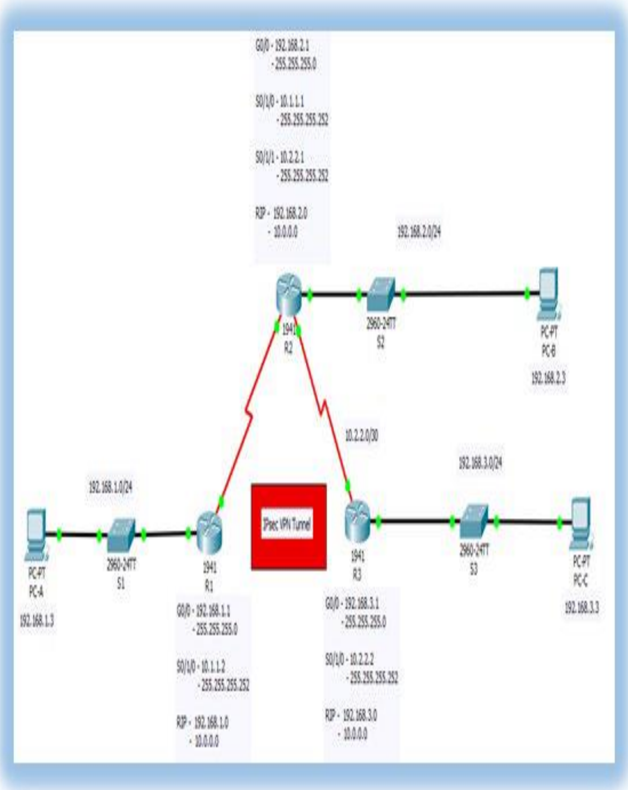


Fig. 3 Topology – VPN Site-to-Site IPsec

<u>Router 1 - IP Address Configuration</u>

```
Router(config-if)#exit
Router(config)#hostname R1
R1(config)#int G0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int se0/0/0
R1(config-if)#ip address 10.1.1.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

<u>Router 2 - IP Address Configuration</u>

```
Router>en
Router#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int G0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int Se0/0/0
R2(config-if)#ip add 10.1.1.1 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int se0/0/1
R2(config-if)#ip add 10.2.2.1 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

Router 3 - IP Address Configuration

```
Router>en
Router#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int G0/0
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#int Se0/0/1
R3(config-if)#ip add 10.2.2.2 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
```

PC A - IP Address Configuration

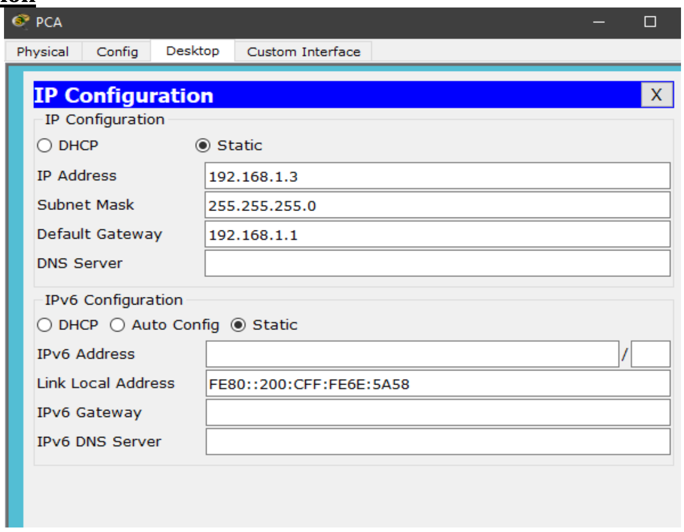


Fig. 4. PC – A IP Address Configuration

PC B – IP Address Configuration

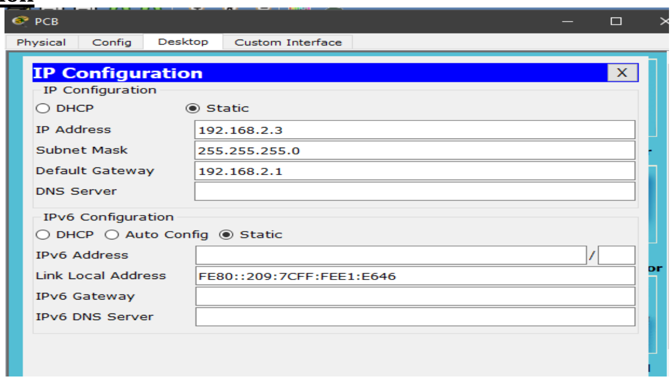


Fig. 5. PC – B IP Address Configuration

PC C – IP Address Configuration

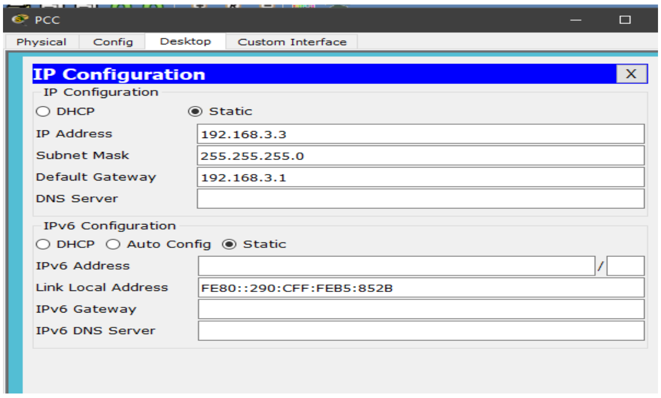


Fig. 6. PC – C IP Address Configuration

Test Connectivity: Ping from PC - A To PC - C

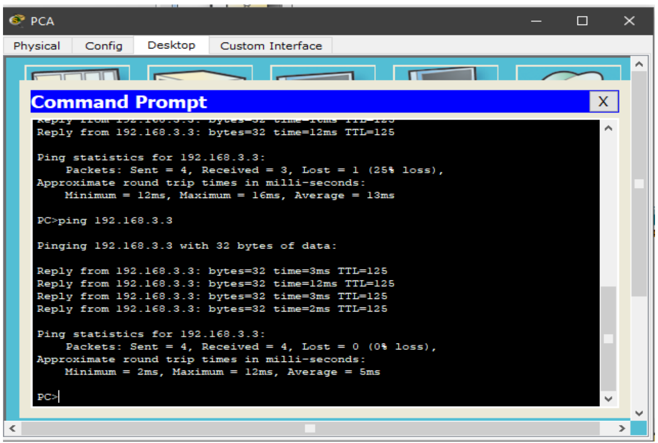


Fig. 7. Test Connectivity PC – A to PC - C

<u>Enable The Security Technology Package On Router R1</u>

```
R1(config)#license boot module c1900 technology-package securityk9
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
```

```
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
Proceed with reload? [confirm]
```

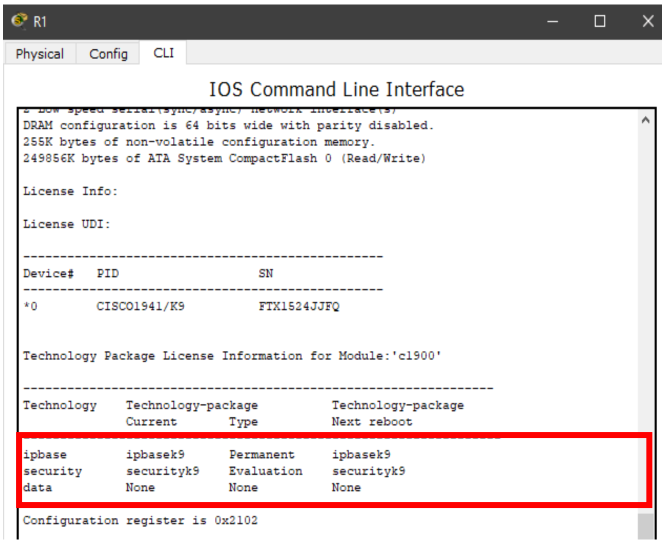


Fig. 8. Router R1 Boot Module Configuration

Identify interesting Traffic on R1

```
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Configure The IKE Phase 1 ISAKMP Policy On R1

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
```

Configure The IKE Phase 2 IPsec Policy On R1

```
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
```

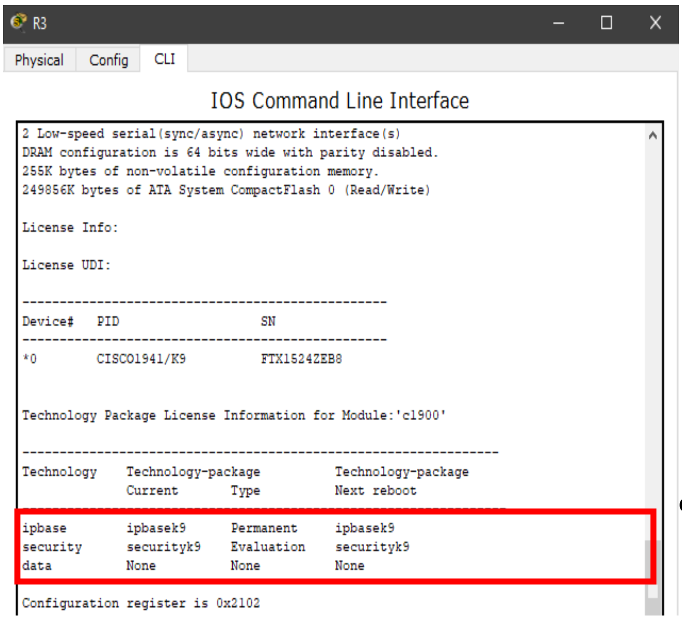
```
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
```

Configure The Crypto Map On The Outgoing Interface

```
R1(config)#int s0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Part 2: Configure IPsec Parameters on Router On R3Enable the Security Technology package

```
R3#config term
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#license boot module c1900 technology-package securityk9
```



```
R1#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    #PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:
```

Fig. 9. Router R3 Boot Module Configuration

Configure Router R3 To Support a Site-To-Site VPN WithR3

```
R3>en
R3#config term
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Configure The IKE Phase 1 ISAKMP Properties On R3

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
```

Configure The IKE Phase 2 IPsec Policy On R3

```
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
```

Configure The Crypto Map On The Outgoing Interface

```
R3(config)#int s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Part 3: Verify The IPsec VPN

Verify The Tunnel Prior To Interesting Traffic

Create Interesting Traffic: Ping PC - C From PC - A

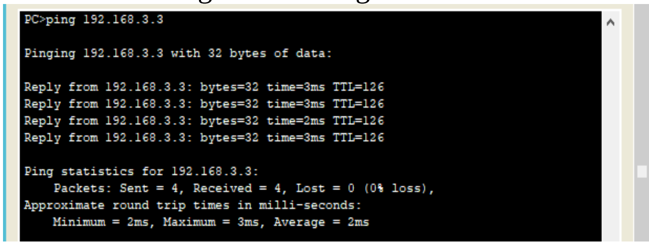
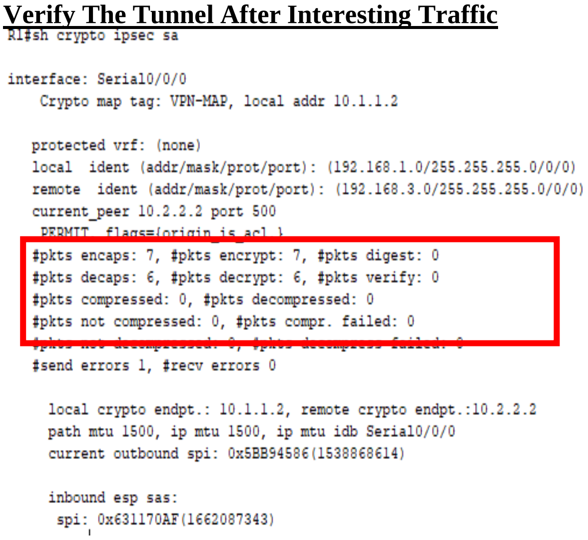

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Fig. 10. PC – Interesting Traffic: Ping PC - C From PC - A

Verify The Tunnel After Interesting Traffic


```
R1#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x5BB94586(1538868614)

     inbound esp sas:
      spi: 0x631170AF(1662087343)
```

<u>Create uninteresting traffic</u>Ping PC - B from PC - A

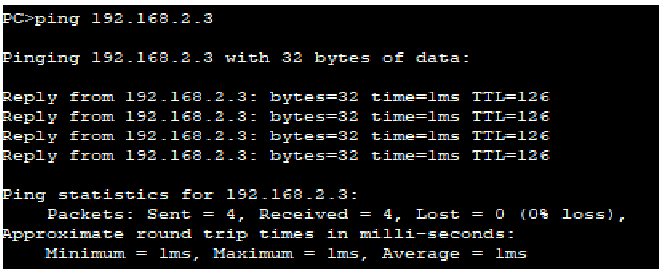

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Fig. 10. PC – Uninteresting Traffic: Ping PC - B From PC - A

Verify the tunnel

```
R1#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x5BB94586(1538868614)

     inbound esp sas:
      spi: 0x631170AF(1662087343)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3519)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
```

Check Results (Ping Test)

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=11ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms
```

Fig. 11. PC – Ping PC - B To PC - A

```
PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=7ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=11ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 5ms
```

Fig. 12. PC – Ping PC - B To PC - C

```
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=10ms TTL=126
Reply from 192.168.1.3: bytes=32 time=11ms TTL=126
Reply from 192.168.1.3: bytes=32 time=11ms TTL=126
Reply from 192.168.1.3: bytes=32 time=7ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 11ms, Average = 9ms
```

Fig. 13. PC – Ping PC - C To PC - A

```
PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=2ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Fig. 12. PC – Ping PC - C To PC – B

V. CONCLUSION

IPsec tunneling has a big important role inenhancing VPNs' security, because it based on thenetwork level, and it is totally hidden in its operation. So, there is no need to learn about it by end users and they never interact with it directly. This is an added security layer for the VPNs running on IPsec.

REFETRENCES

1. Tripti Sharma, Rahul Yadav. (2015). Security in Virtual Private Network. International Journal of Innovations & Advancement in Computer Science, 4(Special issue), 669-675.
2. MohdNazri Ismail and MohdTaha Ismail. (2009). Analyzingof Virtual Private Network over Open Source Application and Hardware Device Performance. European Journal of Scientific Research, Euro Journals Publishing, Inc. 28(2), 215-

226

3. Andrew Mason. (2002). CISCO VPN and VPN technologies. Cisco Press, Retrieved from http://www.ciscopress.com/ articles/article.asp? p=24833&seqNum=6)
4. William Stallings. (2013). Cryptography and network security, Voice Security in Virtual Private Network. Deep Shikha Computer Science and Engineering, ITM University, 3(7).
5. R. Deal (2005). The Complete Cisco VPN Configuration Guide, Published by Pearson Education, Cisco Press.
6. George Dragoi, Ioana Raluca Guica. (2012).The Virtual Enterprise Network based on IPSec VPN Solutions and Management. International Journal of Advanced Computer Science and Applications,3(11), 26-34
7. K. Karuna Jyothi*, Dr. B. Indira Reddy, (2018). Study on Virtual Private Network (VPN), VPN's Protocols And Security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 3(5), 919-932
8. Ritu Malik, Rupali Syal, ―Performance Analysis of IP Security VPN‖, International Journal of Computer Applications Volume 8– No.4, October 2010.
9. Lana Ibrahim. (2017). Virtual Private Network (VPN) Management and IPSec Tunneling Technology. Middle East Comprehensive Journal For Education And Science Publications, 1, 76-87
10. Yang, Y. (2011). Virtual Private Network Management, Bachelor of Information Technology Network Optionion.
11. Muirhead, C. S., & Page, D. J. (2010). U.S. Patent No. 7,684,321. Washington, DC: U.S. Patent and Trademark Office.
12. Snader, J. C. (2015). VPNs Illustrated: Tunnels, VPNs, and IPsec: Tunnels, VPNs, and IPsec. Addison-Wesley Professional.