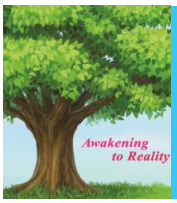

Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 165 (2022) 56195-56199

Elixir
ISSN: 2229-712X

Configuring GRE over IPsec VPN with CertificateAuthority Using GNS3

Vipul Chauhan[1] and Sandeep Rana[2]

[1] M.Tech Scholar in Computer Science, J.P. Institute of Engineering and Technology, Meerut.

[2]Assistant Professor, Department of Computer Science, J.P. Institute of Engineering and Technology, Meerut.

ARTICLE INFO

Article history:

Received: 20 March 2022;

Received in revised form:

20 April 2022;

Accepted: 30 April 2022;

Keywords

VPN,
GRE,
IPSec,
GRE Over IPSec,
CA.

ABSTRACT

There are many protocols which are used to secure the data transfer between the computing devices in a network. Increase in the use of internet is also increasethe demand of security and privacy in a communication and communication channels. To secure the networks there are some protocols which will be used for encryption and authentication for all IP packets of a session. In this research paper will include the advantages and all possible solutions of some techniques which are used to increased security of the network like scalability and data confidentiality. This paper analysis of two most widely used tunneling protocols in secured transmission of data the GRE (Generic Routing Encapsulation) and also the IPSEC (IP Security) established the comparison between them and evaluate the capabilities for security or privacy of the web internet network and for increasingand adding more security and privacy we are going toalso contain and used CA (Certificate Authority) for increasing the network security. We use GNS3 (Graphical Network Simulator 3) for traffic analyses.

Introduction

There are different types of protocols each and every protocol has its own purposes like TCP, UDP, and ICMP etc. IPSec is the type of protocols which supports and transports only unicast packets and GRE is the tunneling protocol which supports and transports multicast or broadcast messages and non-ip packets also. The idea is wrap the data with GRE first and then into IPSec so it is referred to as GRE over IPSec [1]. But now we want to add more security in this we introduce Certificate authority here and add CA into GRE over IPSec It is referred to as GRE over IPSec with CA.

Virtual Private Network (VPN)

VPN is known as a Virtual Private Network. VPN is used for create a secure communication over a public network. There have different types of VPN Protocols like IPSec VPN {S2S (Site 2 Site) and P2P (Point 2 Point)} , Remote VPN , GRE VPN , MGRE VPN , Dm VPN , Get VPN etc. A VPN establishes a secure, encrypted connection between your computer and the internet, providing a private tunnel for your data and communications while you use public networks [2].

Generic Routing Encapsulation (GRE)

GRE is known as a Generic Routing Encapsulation. It is a tunneling protocol initially developed by -CISCO. Main purpose of GRE is to encapsulate wide variety of protocol types inside IP tunnel. It creates virtual point to point link over an internet. GRE is a stateless protocol there is no control flow mechanism. GRE doesn't provide security. It encapsulates the packet by adding additional GRE header of 24 bytes. Mainly GRE is used when we need to form a tunnel between end points for video or voice traffic which used Multicast communication. GRE is the Layer 3 protocol. GRE uses IP Protocol Number 47. GRE is defined as an IETF Standard (RFC 2784) [3].

Internet Protocol Security (IPSec)

IPSec is known as Internet Protocol Security. IPSec provides privacy, integrity, and authentication of information. IPSec support two modes first one is tunnel mode and the second one is transport mode. In the tunnel mode – entire packet is encapsulated and transport mode – only payload is protected. IPSec ESP is defined in RFC2406 [5].IPSec uses IP protocol number 50 for ESP and IP protocol number 51 for AH. Sometime in addition IPSec use UDP port no. 500 for IKE negotiation.

GRE over IPSec

IPSec can't encapsulate multicast, broadcast, or non- IP packets, and GRE can't authenticate and encrypt packets. By means of the GRE over IPSec technology, multicast and broadcast packets can be encapsulated using GRE and also the encrypted using IPSec [6].

Certificate Authorities

CA is known as Certificate Authority. CA is a company or organization that acts to validate the identities of entities and bind them to cryptographic keys through the issuance of electronic documents called Digital Certificates. A digital certificate is providing Authentication, Encryption and Integrity. Authentication is used for serving as a credential to validate the identity of the entity that is issued to and Encryption is used for secure communication over insecure network and Integrity is used for document signed with the certificate so that they can't be altered by a third party in transition.

Routing and Routing Protocols

Routing is a process of sending a packet from one network to another network. Routing has two types Static routing and dynamic routing. Static Routing needs to give all

Tele:
E-mail address: vipul.ch431@gmail.com,

configurations manually. In dynamic routing we have three categories in routing protocols. First one is Distance Vector Routing Protocol, Second is Link State Routing Protocol and the third is Hybrid Routing Protocol.

In, Distance Vector Routing Protocol contains RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol)

Link State Routing Protocol contains OSPF (Open Shortest Path First) and ISIS (Intermediate System To Intermediate System) Hybrid Routing Protocol contains EIGRP (Enhance Interior Gateway Routing Protocol)

Table 1. Comparison of Routing Protocols

Various Routing Protocols					
Features	**RipV1**	**RipV2**	**IGRP**	**OSPF**	**EIGRP**
Classful/ Classless	Classful	Classless	Classful	Classless	Classless
Metric	Hop	Hop	Composite (BW & Delay)	Cost 100,000/BW	Composite (BW & Delay)
Periodic Advertisement	30 Sec	30 Sec	90 Sec	None	30 Sec
Advertising Address	255.255.255.255 (Broadcast)	224.0.0.9 (Multicast)	255.255.255.255 (Broadcast)	224.0.0.5 & 224.0.0.6 (Multicast)	224.0.0.10 (Multicast)
Administrative Cost	120	120	100	110	Internal:90 External:170
Category	Distance Vector	Distance Vector	Distance Vector	LinkState	Hybrid

Tunnel

Tunnel is a way to move packets from one network to another network.Tunneling using a method which is known as Encapsulation. Tunneling is also known as Port Forwarding.

When data is tunneled, it is split into smaller parts called packets, as it travels through the tunnel. The packets are encrypted via tunnel, and another process takes place known as encapsulation. There are various types of protocol that allowed tunneling i.e. Point 2 Point tunneling protocol (PPTP) & Layer 2 tunneling protocol (L2TP).

Implementation

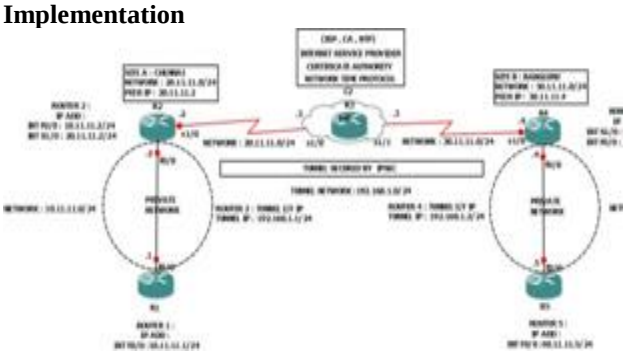

Figure 1. GRE over IPSec implementation B/W two sides using CA

Aim is to make a GRE over IPSec VPN using Certificate Authority because we wantto added more security on Scenario. So, we have two sites and we give configuration on all routers and after complete norma configuration then weuse configuration of GRE VPN and IPSec VPN which is also called GRE over IPSec VPN configuration. Then we use CA for gave digital certificates to the router for providing more security. So we configure the entire CA configuration into the routers.

Configurations

A. Router 1 – Configuration R1#

R1#confi t R1(config)#int f0/0
R1(config-if)#ip add 10.11.11.1 255.255.255.0 R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 10.11.11.2

B. Router 2 – Configuration

R2#
R2#confi t R2(config)# R2(config)#int f0/0
R2(config-if)#ip address 10.11.11.2 255.255.255.0
R2(config-if)#no shutdown R2(config-if)#exit R2(config)#int s1/0
R2(config-if)#ip address 20.11.11.2 255.255.255.0
R2(config-if)#no shutdown
R2(config)#ip route 30.11.11.0 255.255.255.0 20.11.11.3
R2(config)#clock timezone IST 4
R2(config)#do clock set 18:26:00 20 august 2021
R2(config)#ntp server 20.11.11.3
R2(config)#ntp authentication-key 123 md5 cisco
R2(config)#ntp trusted-key 123
R2(config)#ip domain name cisco.com
R2(config)#crypto key generate rsa modulus 1024
2(config)#crypto pki trustpoint cas
R2(ca-trustpoint)#enrollment url http://20.11.11.3
R2(ca-trustpoint)#revocation-check none R2(ca-trustpoint)#exit R2(config)#crypto pki authenticate cas yes
R2(config-if)#exit
R2(config)#crypto pki enroll cas Password:
Re-enter password:
yes no yes
R2(config)#crypto isakmp policy 10 R2(config-isakmp)#authentication rsa-sig R2(config-isakmp)#encryption 3des R2(config-isakmp)#hash md5
R2(config-isakmp)#group 2 R2(config-isakmp)#exit
R2(config)#crypto isakmp key cisco123 address 30.11.11.4
R2(config)#crypto ipsec transform-set tset esp- 3des esp-md5-hmac
R2(cfg-crypto-trans)#exit R2(config)#crypto ipsec profile gre-profile R2(ipsec-profile)#set transform-set tset R2(ipsec-profile)#exit R2(config)#interface tunnel 10
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#tunnel source 20.11.11.2
R2(config-if)#tunnel destination 30.11.11.4
R2(config-if)#tunnel protection ipsec profile gre- profile
R2(config-if)#tunnel mode ipsec ipv4 R2(config-if)#exit
R2(config)#ip route 40.11.11.0 255.255.255.0 tunnel 10
R2(config)#do sh crypto isakmp sa R2(config)#do sh crypto ipsec sa

C. Router 3 – Configuration R3#

R3#confi t R3(config)#int s1/0
R3(config-if)#ip add 20.11.11.3 255.255.255.0 R3(config-if)#no shutdown
R3(config-if)#exit R3(config)#int s1/1
R3(config-if)#ip add 30.11.11.3 255.255.255.0 R3(config-if)#no shutdown
R3(config-if)#exit R3(config)#clock timezone IST 4

R3(config)#do clock set 18:26:00 20 august 2021
R3(config)#ntp master 1
R3(config)#ntp authentication-key 123 md5 cisco
R3(config)#ntp trusted-key 123
R3(config)#crypto key generate rsa modulus 1024 label cas
R3(config)#ip http server R3(config)#crypto pki server cas
R3(cs-server)#issuer-name CN=SA OU=CNS COUNTRY=INDIA L=MEERUT
R3(cs-server)#grant auto R3(cs-server)#no shutdown
Password:
Re-enter password:
% Certificate Server enabled. R3(cs-server)#

D. Router 4 – Configuration R4#

R4#confi t R4(config)#int s1/0
R4(config-if)#ip add 30.11.11.4 255.255.255.0 R4(config-if)#no shutdown
R4(config)#int f0/0
R4(config-if)#ip address 40.11.11.4 255.255.255.0
R4(config-if)#no shutdown R4(config-if)#exit
R4(config)#ip route 20.11.11.0 255.255.255.0 30.11.11.3
R4(config)#clock timezone IST 4
R4(config)#do clock set 18:26:00 20 august 2021
R4(config)#ntp server 30.11.11.3
R4(config)#ntp authentication-key 123 md5 cisco R4(config)#ntp trusted-key 123
R4(config)#ip domain name cisco.com
R4(config)#crypto key generate rsa modulus 1024
R4(config)#crypto pki trustpoint cas
R4(ca-trustpoint)#enrollment url http://30.11.11.3
R4(ca-trustpoint)#revocation-check none R4(ca-trustpoint)#exit
R4(config)#crypto pki authenticate cas yes
R4(config)#crypto pki enroll cas Password:
Re-enter password:
yes no yes
R4(config)#crypto isakmp policy 10 R4(config-isakmp)#authentication rsa-sig R4(config-isakmp)#encryption 3des R4(config-isakmp)#hash md5
R4(config-isakmp)#group 2 R4(config-isakmp)#exit
R4(config)#crypto isakmp key cisco123 address 20.11.11.2
R4(config)#crypto ipsec transform-set tset esp- 3des esp-md5-hmac
R4(cfg-crypto-trans)#exit R4(config)#crypto ipsec profile gre-profile R4(ipsec-profile)#set transform-set tset R4(ipsec-profile)#exit R4(config)#interface tunnel 10
R4(config-if)#ip address 192.168.1.2 255.255.255.0
R4(config-if)#tunnel source 30.11.11.4
R4(config-if)#tunnel destination 20.11.11.2
R4(config-if)# tunnel protection ipsec profile gre- profile
R4(config-if)#tunnel mode ipsec ipv4
R4(config-if)#exit
R4(config)#ip route 10.11.11.0 255.255.255.0 tunnel 10
R4(config)#do sh crypto isakmp sa R4(config)#do sh crypto ipsec sa

E. Router 5 – Configuration R5#

R5#confi t R5(config)#int f0/0
R5(config-if)#ip address 40.11.11.5 255.255.255.0
R5(config-if)#no shutdown R5(config-if)#exit
R5(config)#ip route 0.0.0.0 0.0.0.0 40.11.11.4

Results

Figure 2. Route of Router 1 and Ping from R1 to R5 of Site A to Site B

Figure 3. Route of Router 2

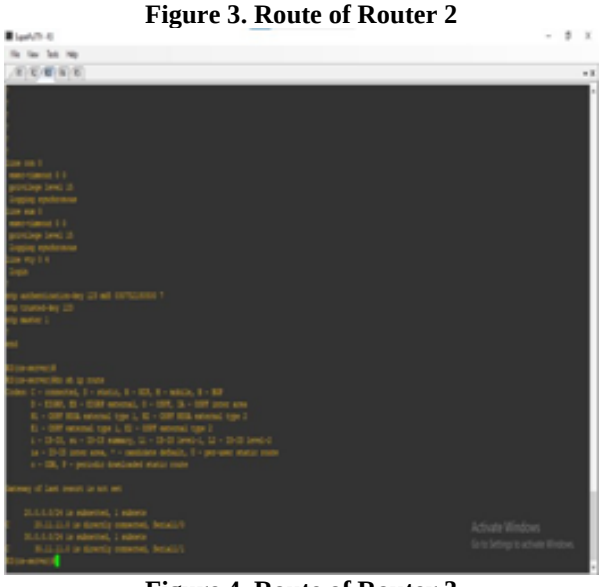

Figure 4. Route of Router 3

Figure 5. Route of Router 4

Figure 6. Route of Router 5 and Ping from R5 to R1 via Site B to Site A

Figure 7. Router 2 Crypto Isakmp & IPSec Details

Figure 8.Router 2 IPSec Details

Figure 9. Router 2 IPSec Details

Figure 10. Router 4 Crypto Isakmp & IPSec Details

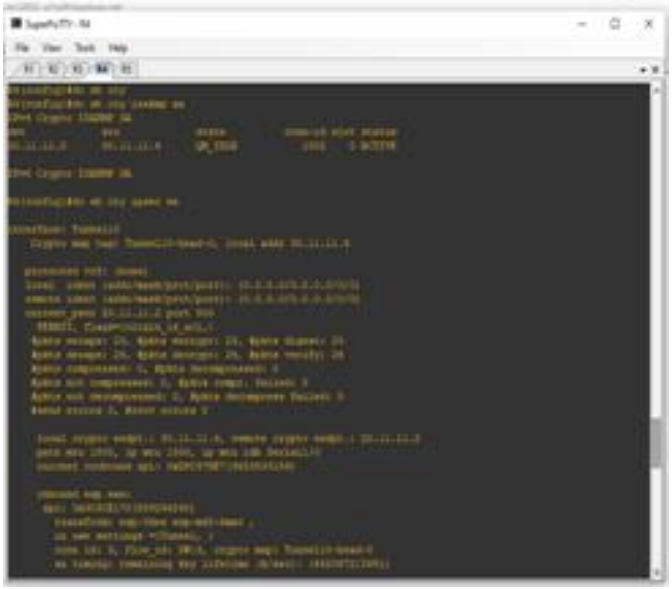

Figure 11. Router 4 IPSec Details

Figure 12. Router 4 IPSec Details

Conclusion

In this Research Paper we have discussed about the VPN, GRE VPN, IPSec VPN, Tunneling, Routing and Routing Protocols, CA, GRE over IPSec and we have shown how we secure the transmission of non IP packets traffic or either we say Transmission of multicast Packets through the IPSec using GRE Over IPSec and providing more security and privacy assurance by using and adding Digital Certificates by Certificate Authorities using GNS3 along with the configurations.

References

[1]. Dr J SEBASTIAN NIXON , Dr A FRANCIS SAVIOUR DEVARAJ and MAHFUZ ABDELKADIR MOHAMMED ijesird, Vol. III, Issue II, August 2016/112
[2]. https://www.avast.com/c-what-is-a-vpn
[3].https://www.ciscopress.com/articles/article.asp?p=2832406&seqNum=7#:~:text=1.2)-,GRE%20is%20a%20tunneling%20protocol%20developed%20by%20Cisco%20that%20can,a%20single%2Dprotocol%20backbone%20environment.
[4]. https://surfshark.com/learn/what-is-vpn
[5]. https://ipwithease.com/gre-vs-ipsec/
[6].https://support.huawei.com/enterprise/en/doc/EDOC1100055047/62c5ea60/gre-over-ipsec
[7].https://www.ssl.com/faqs/what-is-a-certificate- authority/
[8].https://www.techopedia.com/definition/5402/tunneling#:~:text=Techopedia%20Explains%20Tunneling-What%20Does%20Tunneling%20Mean%3F,through%20a%20process%20called%20encapsulation.