Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

Security for Cloud Data Protecting by VPN

A
Dissertation Report
Submitted to
Mewar University, ChittorgarhTowards the
partial fulfillment of The Degree of
Master of Technology
In Computer Science & Engineering

Submitted To:
Mr. B. L. Pal
HoD
Computer Science & Engineering

Submitted By:
Ravi Ranjan Kumar
MUR2103922

Faculty of Engineering & Technology Department of Computer Science
& EngineeringMewar University
Chitorgarh (Rajasthan) Year of
Submission 2024

ABSTRACT

Context: From the past few years, there has been a rapid progress in Cloud Computing. With the increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users using centralized resources. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user.
Aims and Objectives: The main aim of this research is to understand th`e security threats and identify the appropriate security techniques used to mitigate them in Cloud Computing.
The main objectives of this research are:
To understand the security issues and the techniques used in the current world of Cloud Computing.
To identify the security challenges, those are expected in the future of Cloud Computing.
To suggest counter measures for the future challenges to be faced in Cloud Computing.
Cloud computing offers enterprises a method to access computing resources on-demand. This allows enterprises to save on capital expenses related to periodichardware upgrades, maintenance and energy costs. However data traversing in cloud, leads to data breaching and data loss by third party intruders affecting the managing and reliability of sensitive information. A virtual private network, VPN, is a typical way of interconnecting networks over a public network infrastructure securing data transferred across the private subnets. The goal of this project is to provide VPN as a service using virtualized VPN software, essentially making the VPN yet another building block for a service in the cloud.
Objectives: The objective of this thesis involves the modeling of an open source IPSec based VPN solution on a Linux Platform and estimating its performance efficiency for implementing VPNaaS prototype. Also resource allocation and management metrics are evaluated to determine the rate and reliability of launching VMs. An extensive literature review has been carried out depicting the various VPN implementations and various security enhancing key distribution mechanisms.
Methods: Configuration and modeling of an IPSec VPN solution on a Linux environment has been accomplished by proper experimental set-up in the FIWARE federated cloud where performance metrics on throughput, jitter and packet loss were measured and analyzed. Overheads concerning various encryption algorithms have been studied and resulted.

Results: AES128-MD5 outperforms all the other algorithmic combinations, owing to its advanced functionality and software compatibility. TCP and UDP analysis show comparative analysis between tunnel and non-tunneled traffic. VM resource allocation, failure ratio and service operational times were also measured to evaluate factors like speed and reliability of VPN services.

Conclusion: Introducing VPN prototype to the cloud can enable cloud users to remain interconnected across multiple geographical locations simultaneously enhancing data integrity and confidentiality. Thorough literature review conducted on various VPN architectures, key distribution mechanisms will supplement future researchers to select accurately depending on pre-requisites. There is also a lot of scope for future work, including various caching algorithms for overhead reduction enhancing performance efficiency.

- ***Keywords*: Cloud, Challenges, Computing, Security, StrongSwan, Virtualization, VPN.**

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

CONTENTS

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

LIST OF FIGURES

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

ABBREVIATIONS

AES	Advanced Encryption Standard
AH	Authentication Header
API	Application Program Interface
AS	Autonomous System
CA	Certificate Authority
DOA	Dead On Arrival
ESP	Encapsulation Security Payload
FTP	File Transfer Protocol
GE	Generic Enabler
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange Protocol
IKEv1	IKE version 1 Protocol
IKEv2	IKE version 2 Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol MD5 Message Digest Algorithm
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Card
PPTP	Point-to-point Tunneling Protocol
PSK	Pre-Shared Keys
SA	Security Association
SHA	Secure Hash Algorithm
SPI	Security Parameter Index
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
3DES	Triple Data Encryption Standard
UDP	User Datagram Protocol
VM	Virtual Machine
VMM	Virtual Machine Monitor
VNF	Virtualized Network Function
VPN	Virtual Private Network
VPNaaS	Virtual Private Network as a Service

1 INTRODUCTION

In contrast to the past, where the dependence on physical computing storage or serversfor running programs was significant, the introduction of cloud computing has replaced accessing of data and programs across the Internet for big business enterprises, firms and entrepreneurial institutions. Opting for the cloud helps organizations save up on money and human resources as it eliminates the need for investment into computing hardware, storage and other physical infrastructure. This reduces the inconveniences of operating large systems, related technical problems, as well as backup issues. Software as a service is acloud service, where software functionalities are provided as a service. Few of its key features include scalability, data management and customizability [1].

Virtualization is a key aspect of cloud computing [2] as it simplifies the delivery of services by creating a layer of abstraction hiding the complexity of underlying hardware, decoupling the software and hardware, hereby supporting resource scalability andcontributing in making the cloud cost effective. The three important characteristics of virtualization [3] making it ideal for the cloud are: partitioning, isolation and encapsulation. Partitioning in virtualization allows parallel processing of multiple Virtual Machines (VMs) on a single physical system. Isolation among VMs ensures the data integrity and program execution on specific VM is not compromised by outside VMs. Encapsulation is the abilityto represent each VM as a single file or a set of related files, meaning that the state of VM can be saved to a file system and can be easily copied or moved to a remote host. Hypervisors are considered core components of a virtualization platform. The main responsibility of the hypervisor is to delegate computer hardware to Virtual Machine Monitors. Running multiple VMs simultaneously on a single compute node, helps in effective utilization of hardware [4]. Thus providing VPN to the cloud, help in cost effective savings, simplified management and enhanced security.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

A VPN spawns a private network using the private IP space between multiple sites connected over the Internet. Encryption and cryptographic protocols can be used to provide confidentiality, integrity and authentication of the user data transmitted over the Internet [5]. Many corporations cannot accept that their important and confidential data be placed in public cloud, which is a cloud managed by an entity outside the corporation control. A private cloud gives users a flexible and agile private infrastructure to run service workloads within their own administrative domains. One way to ease the adoption of public clouds by corporations is to connect cloud VMs to the corporation network using a Virtual Private Network (VPN) [6]. For securing data communication over the unreliable public Internet, SSL, IPSec, and PPTP are the three commonly used protocols for building VPNs [7]. Since IPSec-based VPNs are not application dependent, they are chosen for site-to-site VPNarchitecture in this research over application dependent protocols. IPSec is also considered ideal for monitoring and securing inbound and outbound Internet traffic [8].
Site-to-site IPSec-based VPN tunnels are set-up across the FIWARE federated cloud lab. Launching, deploying and managing of VM resources are enabled through the FIWARE GUI or OpenStack command-line interface. To ensure data security through encryption and authentication algorithms, *strongSwan*, an open source Linux-based IPSec VPN solution is implemented to ensure data confidentiality against third party intruders.

1.1 BACKGROUND

The Internet Engineering Task Force (IETF) provides the standardized definitionof a VPN [9]; “A network in which connectivity among multiple private Wide Area. Networks (WANs) is deployed using shared IP infrastructure with the same policies as aprivate network.”

A VPN connection includes the following components:

- **VPN gateways:** A VPN peer which initiates/accepts traffic from a correspondingVPN peer.
- **VPN Tunnel:** The portion of the connection in which the traversing data isencapsulated.
- **VPN connection:** The portion in which the traversing data is encrypted.

A VPN is constructed following different architectural structures which are described indetail in the succeeding sections.
Despite the benefits of shifting to the cloud, data breaching, data loss and traffic hijacking are rated among the top threats to cloud computing security [10]. Extraction of private cryptographic keys and sensitive information, false data injection and data manipulation are few vulnerabilities that are to be handled through secured transmission of data with proper VPN management. Various security breaches such as Man in the Middle attack, Distributed Denial of Service attack have raised the necessity of an effective VPN solution in the cloud.
Among different methods, encryption of data is considered extremely helpful in assuring data protection within a cloud-based environment [11]. Thus this drawback of cloudsecurity is overcome in this paper, by deploying VPN services in the cloud to ensure data protecting and confidentiality of sensitive information. Few advantages of moving VPNs to the cloud are the security enhancements provided to users. Central management and flexibility in terms of third party data manipulation and provision of integrated security policies providing superior protection are of at most importance.

1.1.1 Problem Statement

Cloud computing offers a way for enterprises to access computing resources on- demand. This allows enterprises to save on capital expenses related to periodic hardware upgrades, maintenance and energy costs. Furthermore, cloud computing enables enterprises to dynamically allocate and/or release resources to match their needs or the demand from their customers. Many cloud providers have built data centers in various geographic locations and interconnected them through high-speed Internet links. This makes it possible for cloud tenants to instantiate services close to the location of the users. Theoretically, a customer can rent resources from several cloud providers and merge them together in a common pool, as is the case in a federated cloud.
The resources in the pool are often building blocks for services, typically VMswith associated memory, storage and network. These building blocks, denoted as Virtual Network Functions (VNFs) or Generic Enablers (GEs), are interconnected into servicechains that can do advanced data processing. In a federated cloud the interconnected elements can span vast geographic distances as well as multiple Internet Autonomous Systems (ASs).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

Considering a scenario wherein various cloud providers are involved, each providing different services such as online shopping, web services and so on. Tenants as a part of either of the cloud, do not want their card credentials to be compromised when associated with the shopping services. Similarly, tenants with business relations do not want their confidential data to be compromised in transit. For similar reasons, Cloud tenants, not wanting to rely on cloud provider services, can build their own private VPN tunnel forsecure transfer of information.
In this situation it is desirable that data traversing these elements remains confidential and that third parties cannot alter it without detection. In addition, it is often convenient that chain elements instantiated with different providers are located in a common IP address space. This can simplify the implementation of service discovery, load balancing, high-availability schemes etc.
A VPN is a typical way of interconnecting networks over a public network infrastructure. Although several cloud providers offer VPN access to their tenants this can beundesirable in certain circumstances (e.g., the tenant does not trust the provider and/or the tenant wants to have better controls over the VPN policies and key generation and distribution process). The goal of this project is to provide VPN-as-a-Service (VPNaaS) using virtualized VPN software, essentially making the VPN yet another building block for aservice.

1.2 Research Questions

The project will investigate the following research questions:

	Research Questions
RQ1	What architectures are suitable for implementing virtual VPN?
RQ2	What are the various methods used for key distributions in enabling the security of the network?
RQ3	How to design an IPSec based VPN solution in an virtualized environment?
RQ4	What are the performance impacts on the operation of the VPN in cloud?

1.3 Research Contribution

The thesis focuses on establishing a Linux-based virtualized environment facilitating communication between the VMs running in a cloud. An important part of this project was the configuration and implementation of an open source IPSec VPN solution using *strongSwan.* In addition, a detailed study was conducted on the various architectural choices for building a VPN such as site-to-site, host-to-host and remote access VPNs,Various key distribution mechanisms for enhanced security through are discussed withemphasis on specific features. Performance metrics like throughput, jitter and packets lossfor TCP and UDP packets are analyzed and implications are briefed. There is an also an investigation of the overheads related to tunneled as well as non-tunneled traffic. Conclusions are drawn based on the results analyzed and scope for future study is also mentioned.

1.4 Document Outline

Chapter 2 emphasizes on the background study undertaken to substantiate valid research in this paper. Analyses of various VPN software packages for different operating systems such as Windows and Fedora, IPSec VPN performance analyses relating to different metrics are studied concisely. Various overheads introduced due to specific encryption algorithms have also been reviewed.

Chapter 3 deals with the functionalities and operation of IPSec VPNs enhancing IKE ESP characteristics, various security enhancing key distribution techniques including Pre-shared keys and comparative analysis on different VPN architectures.

Chapter 4 gives an overview of the experimental set-up and configuration details are recorded. The requirements to offer VPN as a VNF have also been mentioned.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

Chapter 5 concentrates on the measurements performed by analyzing different encryption algorithms for tunneled and non-tunneled traffic graphically illustrating them. VM provisioning time, VM Failure Ratio and VPN service start up time have also been measuredto gain insight into the speed and reliability of resource allocation.

Chapter 6 emphasizes on analysis of the recorded results. It explains in detail the reasons for throughput and jitter performance among TCP and UDP packets across tunneled and non- tunneled traffic.

Chapter 7 concludes with various scientific deductions, answers the research questions and also provides scope for future work.

2 RELATED WORK

The body of related work described in this section provides details and statistical insights beneficial for this research.

2.1 OpenVPN Analysis

Berry Koekstra and Damir Musulin in [12] demonstrate the differences in loss of network performance conducted on OpenVPN with different parameters such as encryption algorithms, hashing algorithms and MTU values for measuring network throughout. Authorsin [12], calculated the theoretical network throughput by means of OpenSSL file-based encryption and the practical values on OpenVPN with many iperf measurement tests. Resultsindicated that OpenVPN was unable to attain the same throughput as expected from OpenSSL speed tests and induced an overhead of 75%. Since the encryption algorithms wereinitially considered to be the cause of loss in network throughput, different encryption algorithms were considered to rule out the possibility of inefficient encryption algorithms. The maximum gain in performance was observed to be 150% for Blowfish-128-CBC and 30to 80% for AES ciphers in comparison to the practical OpenVPN measurements. It is also observed that increase in MTU values facilitated an increase in network throughput.
The work in this report focuses on the performance analysis of various algorithms at variable MTU sizes with *strongSwan* solution accounting to the cloud.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

2.2 IPSec performance on Fedora and Windows Operating Systems

Authors in [13] concentrate on the IPSec VPN throughput analysis carried out on Fedora 15 OS and [14] performs similar throughput analysis on Windows 7 OS. Varied combinational systems of encryption and hashing algorithms were compared on both OSs such as DES-MD5, AES128-SHA, and 3DES-SHA etc. The clients across the site-to-site architecture were connected in a wired and wireless scenario.

On Windows operating system, AES128-SHA delivered the best UDP functionality and 3DES-SHA system exhibited superior TCP performance whereas on Fedora AES192-SHA exhibited higher UDP results and DES-MD5 performed better with higher TCP results. Superior performance was observed in UDP throughputs in comparison to TCP because being a connectionless protocol UDP does not use any form of errorcorrection and hence does not send acknowledgments. It was also observed that the TCP throughput increased as the packet size increased.

Current research deals with site-to-site VPNs in the cloud framework, exhibiting identical throughput analysis indicating that TCP throughput increases with increase inpacket size. Research in this paper, includes TCP and UDP analysis for tunneled and non- tunneled traffic giving insights into overhead analysis on the cloud platform.

2.3 IPSec complexities

As stated by Shreyas Srivatsan et al. in [15], IPSec causes configuration complexity and inconsistent implementations. Despite having the advantage of operating transparently to applications in the host system, the complexity of the protocol has led to interoperability problems between systems. The main reason for complexity is the usage of multi-purpose certificates in public key authentications [15]. Thus [15] presents an IPSec configuration compiler, Simple-VPN to tackle these IPSec complexities. Simple-VPN generates authorization only certificates limited to the machine that is a part of the VPN, rather than to the identity of the user. The compiler has been designed to support cross-

platform implementations, flexibility to end-users by substantiating useful extensions and compatible to the addition of new IKE features. This paper provides an insight into the complications involved with the utilization of public key authentication in the form of digital certificates for IPSec VPN implementations.

Current research focuses on the avoidance of complexities in the cloud, thusfocusing on Pre-Shared Key authentication for key distribution to yield better VPN performance in cloud also giving a detailed literature review on the various key distribution mechanisms available.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

2.4 Analysis of Encryption Algorithms on site-to-site VPNs

The authors in [16] implement a site-to-site VPN on Cisco routers in a Windows Vista environment giving an explanation of how VPN performance is affected hinging on to the optimal selection of different encryption algorithms. Among the different combinationsof encryption, AES256 and 3DES, and hashing algorithms, SHA1 and MD5, used AES256- MD5 system displayed the best throughput performance in comparison to the others. Furtherdeduction revealed that AES256 performed better that 3DES and MD5 superior to SHA-1. This paper comprehends the need for optimal algorithm preference to obtain higher network throughput.
Likewise, the current research yields similar outputs, stating AES algorithms with different block sizes perform better than 3DES while MD5 outperforms SHA but in a Linux-based environment on a cloud infrastructure.

2.5 Performance evaluation of software VPNs

Joseph Evans *et al.* in [17] presents the performance observed on software VPN such as FreeS/WAN, PPTP etc. in terms of network throughput and CPU usage under two main cases consisting of fast (100Mb/s) and slow (10.3kb/s) network. It is observed that when the network connection is fast, the transference speed could degrade to 65% and the CPU usage reached up to 97%, when strong encryption is enabled. Over a low speed network, it was observed that CPU usage was not significantly affected by the VPN. Furthermore, when compression was enabled without overhead network throughput could beincreased.

2.6 Performance Evaluation of Remote Access VPNs

Experimental analysis conducted with *strongSwan* client and IOS IPSec gateway show reduction in the flow rates with increased jitter, latency and packet loss as stated in [18]. The above measurement results are more pronounced in high-speed transmissions and are negligible at lower speeds. It is observed that the loss of performance with IPSec VPN connection is the result of overheads, which encourages the additional IPSec headers, as well as processor complex cryptographic operations that are executed over packages on the client and the gateway [18].
This report achieves similar results when measurements are conducted across tunneled and non-tunneled traffic. It is observed that jitter increases in comparison to non- tunneled traffic, due to additional IPSec headers and complex algorithmic operations.

2.7 Analysis of IPSec overheads for VPN servers

The authors in [19] evaluate the performance overheads of IPSec VPN through the implementation of an open source IPSec VPN software called *OpenSwan*. The author's focuson the tunnel mode of operation and Encapsulation Security Payload protocol because it is widely deployed configuration for building VPNs. In order to analyze the performance impact of various IPSec component protocols, Internet Key Exchange (IKE) and

Encapsulation Security Payload (ESP), as well as various encryption and cryptographic key sizes, the authors utilized two methods. One method measures the run times for individual security operations and the second method replaces various IPSec components with no-ops and records the speed-up in run times of various IPSec phases. It is observed that overheads of IKE protocol are higher than ESP during processing of data packets where cryptographic operations contribute to 32-60% of IKE and 34-55% of ESP protocol [19].
Thus to summarize, estimation of overheads is necessary for evaluating the performance efficiency when using VPNaaS.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

3 IPSEC VPN ASSOCIATIONS

This chapter explains in detail what the IPSec protocol suite consists of, its features and functionalities, followed by the various key distribution mechanisms that can be adopted for deployment in the cloud and the different VPN architectures suitable for implementation in the cloud.

3.1 IPSec

IPSec is a protocol suite for securing Internet Protocol communications by authenticatingand encrypting each IP packet in a communication session [20]. Encapsulation Security Payload, Authentication Header and Internet Key Exchange are the main IPSec protocols used to provide security services. Based on the architectural requirements, IPSec is implemented either on gateway routers or end-hosts.

3.1.1 IPSec Features

Following are the features exhibited by IPSec [21]:

- **Authentication** and **Confidentiality** is provided by encrypting the packets, which when passed over the Internet are in the form of cipher text. Thus eaves dropping by any unknown third party sources renders meaningless since the data-carrying payload is unidentifiable.
- **Data Integrity** verifies that no bit has been modified or manipulated in transit across the end gateways.
- **Anti Replay** ensures IP-packet level security by making it impossible for a third party source to intercept message packets and insert changed packets into the data stream between the end-to-end gateways.
  So an IPSec VPN can be leveraged across the Internet to keep the transmitted data safe and secure.

3.1.2 IPSec Functionality

Traffic sourcing from particular subnet to be transmitted to the destination subnet, instead of only forwarding, the packets are encrypted converted to cipher text and encapsulated. Internet observes packets being transmitted from the router 1 to router 2, whereas packets are being transmitted across the 2 different subnets located on either side of the VPN gateways. (For instance, Any traffic sourcing from 10.1.0.0 network to be transmitted to the destination network of 10.2.0.0 is observed by the Internet to be transmitted from 192.168.0.1 to 192.168.0.2, which are the global address of the VPN gateways enables across the ends). The packet payload is completely encrypted not understandable to eavesdroppers, which is decrypted at the other end and forwarded to the specified destination.

3.1.3 IPSec modes of operation

Tunnel mode and transport mode are the two specific modes of operation defined for IPSec [22].

- In tunnel mode, the original packet including the payload and the header are encapsulated and encrypted by a new set of IP header. The new IP header contains the source and destination of the VPN peer gateways. Packets received at the other end are de-encapsulated and decrypted to obtain the original IP packet, which is thentransmitted to the local network. The benefits of implementing IPSec in tunnel mode

  include its compatibility with VPN gateways, easier NAT traversing ability. Poor interoperability and additional overheads are few drawbacks handles by the tunnel mode.
- Transport mode encrypts only the payload leaving the IP header of the packetunencrypted. The packet payload along with ESP header and trailer are encapsulated. With IPSec transport mode, IPSec encrypts only payload of the packet, theoretically making a copy of the original IP header and attaching it at the starting of the IP secured packet thus exposing the original header. The benefits of implementing IPSec in transport mode include the provision of end-to-end security, lower overhead. Difficulties in NAT traversal and individual IPSec implementations are few issues in this mode.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

3.1.4 Encapsulation Security Payload and Authentication Header

IPSec defines two protocols: AH protocol and ESP. Data encapsulation is providedby these two protocols from the IPSec suite.
The selection between AH and ESP protocols [23] depends on the level of protection necessary for the IP datagrams. The AH protocol provides connectionless integrity, protection against replays, data authentication to all the packet headers and data butdoes not provide encryption of data. Also, AH protocol is not compatible with NAT, since it includes the source and destination IP address in its integrity protection calculations. The ESP protocol, on the other hand, provides data authentication and integrity protection for encapsulated IP packet, as well as data encryption missing in an AH protocol. The ESP tunnel mode is most widely used in IPSec based VPNs because of its ability to encrypt the original IP header, hide the true source and destination of the packet and modify/alter it with the gateway router's IP address [24].
This paper concentrates on the usage of ESP in tunnel mode due to its above- mentioned functionalities and flexibilities.

A brief description on the ESP protocol, its headers and their functionalities are reported forclear understanding:

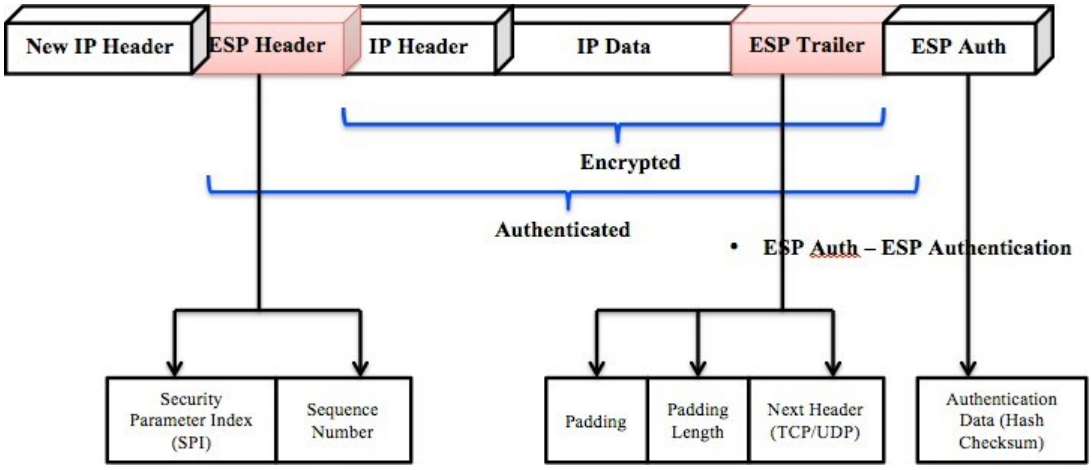


Figure 1: ESP header and field description

ESP provides security by encrypting IP datagrams. An encryption algorithm combines thedata with a key to transform it into encrypted format.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

The ESP protocol contains the following fields [25]:

- ESP header
  Security Parameter Index (SPI): The SPI when used in combination with ESP header and destination address identifies the SA for communication. The responder uses this value to determine the security association with which the packet is identified.
  Sequence number: It is a 32-bit, incrementally increasing number providing anti- replay services to ESP.

- ESP trailer
  Padding: Padding is a functionality used by block ciphers, which require theplaintext to be padded to a multiple of block size.
  Padding Length: Padding Length indicates the length of the padding in bytes.
  Next Header (UDP/TCP): Identifies the type of data in the payload field.

- ESP Authentication data
  Authentication Data: This field consists of the Integrity Check value (ICV), and a message authentication code used to verify the sender's identity and message integrity.

3.1.5 Internet Key Exchange

Even before either AH or ESP protocols are used, the devices need to exchange the"secret", used by the security protocols. The purpose of the Internet Key Exchange protocol is to negotiate, create and manage Security Associations (SA). By default, IKE uses port 500 to transfer series of messages contained in UDP datagrams. Security association is a relationship between two or more entities describing how the security services will be utilized by those entities for secure communications across the networks. Each IPSec connection provides encryption, authentication and integrity to the data transmitted acrossthe network.
When the security association is resolved, the two IPSec peers then determine the encryptionand integrity algorithms to be used (for instance, DES, 3DES, AES256 for encryption and MD5, SHA-256 for integrity) followed by the sharing of session keys between the two IPSecVPN peers [20] [21]. IKE key determination is a refinement of the Diffie-Hellman key exchange algorithm. IKE key determination is designed to retain the advantages of DiffieHellman, while countering its weaknesses.

The IKE key determination protocol is characterized by important features [26]:

- Employs a procedure known as cookies to thwart clogging attacks, clogging attack isa type Denial of Service attack where an intruder tries to cover client resources by creating heavy server or network traffic.
- Enables the two parties to negotiate encryption keys during IPSec associations.
- Enables the exchange of Diffie-Hellman key values.
- Authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

3.2 Key Distribution Mechanisms

According to the current report, security is provided only between gateways (routers, firewalls, etc.) and no host implements IPSec. This illustrates simple VPN support. The security architecture specifies that only a single tunnel SA is needed to achieve this. The

tunnel could support AH or ESP option. The key management portion of IPsec involves thedetermination and distribution of secret keys.
Different authentication methods [21] [27] suitable for enhancing security in the cloud are discussed below:

- Pre-shared key
- Digital signatures

The different methods for authenticating the IPSec-VPN peers are as follows:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

3.2.1 Pre-Shared Keys

Definition: Pre shared keys [21] is string of unicoded characters used in the authenticationof IPSec-VPN entities. The peers use the pre shared keys and nonce (an arbitary number used only once for communication) to create a hash that is used to authenticate messages.

Working: With pre-shared keys, the same pre-shared key is configured on each IPSec peer. During negotiation, information is encrypted prior to transmission using a session key. The session key is created using the Diffie-Hellman calculation and shared secret key. If the receiving peer is able to independently create the same hash using its pre-shared key, then it knows that both peers must share the same secret, thus authenticating the other peer, if not packet is discarded. Pre-shared keys are easier to configure than manually configuring IPSecpolicy values on each IPSec peer.

Example: In IKEv2, negotiation of IKE SAs takes place in two phases. The first phase begins with the exchange of nonce between the two sides, followed by Diffie-Hellman exchange. The two sides then generate a set of IKE keys using the nonce, Diffie-Hellmankey and the pre-shared key. Authentication data is then exchanges, via IKE encryptedmessages. In the second phase, with the exchange of SPI values and possibly another Diffie- Hellman exchange IPSec SAs are generated. Thus encrypted traffic is sent across the two peers after the establishment of IPSec SA.

Advantage: Pre shared keying provides peer-to-peer authentication thus overcoming the disadvantages of other keying mechanisms. PSK also enhances the benefits of using Internet Key Exchange protocol.

Disadvantage: If many users know the PSK, impersonating the gateway is easy and thus not recommendable for large-scale deployments. And also pre-shared keys are stored as plain text in system directories.

3.2.2 Digital Certificates

Definition: A digital certificate [27] is an electronic document that provides authenticationto the public key and validation to the owner's identity. This method forms the basis of authentication for IPSec-VPNs. It is attained from a Certificate Authority, a trusted third party organization.

Working: RSA signatures are used by Certificate Authorities, CAs, which are trusted third- party organizations. An IPSec peer registers itself to the CA to attain a digital certificate. After the CA verifies the peer's credentials, a certificate is issued. A digital certificate consists of the following information:

- The name of the public key holder.
- The name of a party certifying the key indeed belongs to the declared holder.
- The public key itself.
- A digital checksum of the certificate itself encrypted with the private key of the party issuing the certificate.

The agency creating a digital certificate guarantees that the public key belongs to theparty that requests the certificate. The requesting party is the *subject*, and the party issuing the certificate is the *issuer*. The issuing agency creating the certificate collects the information from the subject, confirming the true identity of the requestor. Then the requesting party's name, requesting party's public key and the issuer's own name is combined into a data structure and a digital checksum of the data structure is calculated. The certifying organization encrypts the result of this checksum using its own private key and appends the encrypted checksum to the certificate's data structure. After completing this process anyone is allowed to examine the digital certificate and verify that a certain public key does in fact belong to a specific entity. This authentication method requires complete trust over the certificate-certifying agency.

Example: Assume C is a Certificate Authority issuing digital certificates to two peers A and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

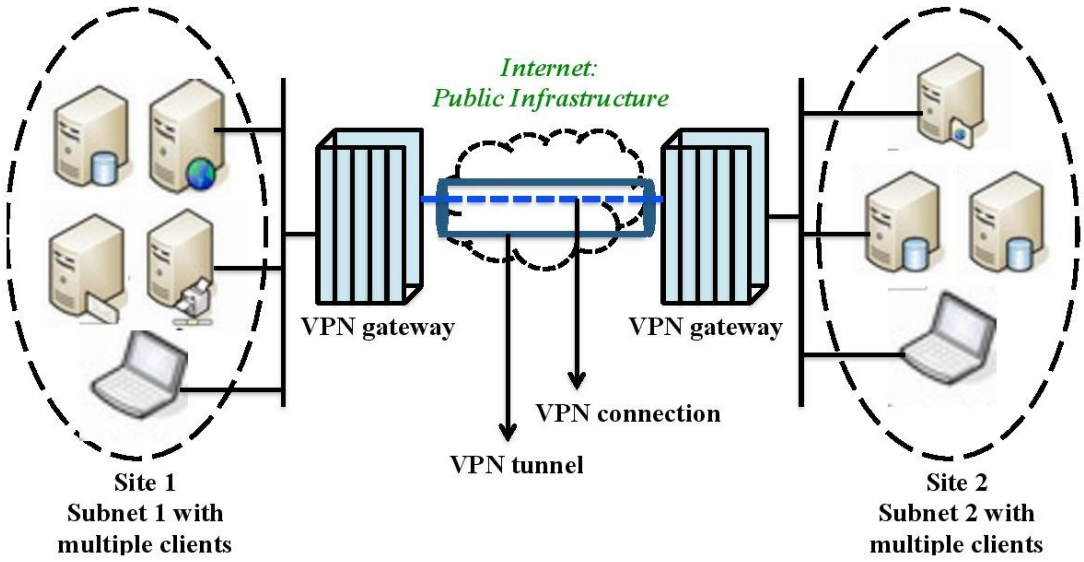
B. A is the subject here requesting the issuer for a digital certificate. C confirms the identity of A by appealing for few A's credentials. Once the issuer, i.e., C is satisfied with the true identity of A, a digital certificate is constructed using a computer program. The input data to this program are A's public key, A's name as the subject and C's name as the issuer. Withthe given data, the computer program calculates a digital checksum over the combination of the above inputs and encrypts it using C's private key. Now B wants A's public key. B locates A's digital certificate and validate it using the public key of the issuer, C.
For validation, B separated the encrypted checksum from the digital checksum and a checksum is calculated on the remaining of the data structure. B then decrypts the original checksum with the C's public key and a comparison between the two checksums is made. If the checksums match, it indicates that C is the true issuer of the certificate containing required information.
The certificate thus issued is self-authenticating because both the peers trust the CA and have their public key available. This authentication method uses X.509 certificates to verify the authenticity of the IPSec peer.

Advantage: Added flexibility. In case a client is compromised client certificate is revoked rather than re-configuring every client.Disadvantage: Certificate-based authentication involves VPN clients and gateways dependent on third party sources also adding additional complexities.

3.3 Comparative Analysis of Different Architectures

There exist different approaches [21] through which the data can be accessedacross a VPN: host-to-host, site-to-site and remote access configurations. Each of their advantages and disadvantages have been studied, to select the best suitable. Site-to-site are built when accessing of data is done across different geographical locations or through different subnets. Host-to-host configurations establish connections between two different hosts initiated by either one. This approach is suitable for communicating to a remote web server or to a backup system. Remote access VPNs are set up usually for connecting from a remote place to the home network in so-called "road-warrior" scenarios.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024



SITE-TO-SITE VPN ARCHITECTURE

Figure 2: Site-to-site VPN architecture

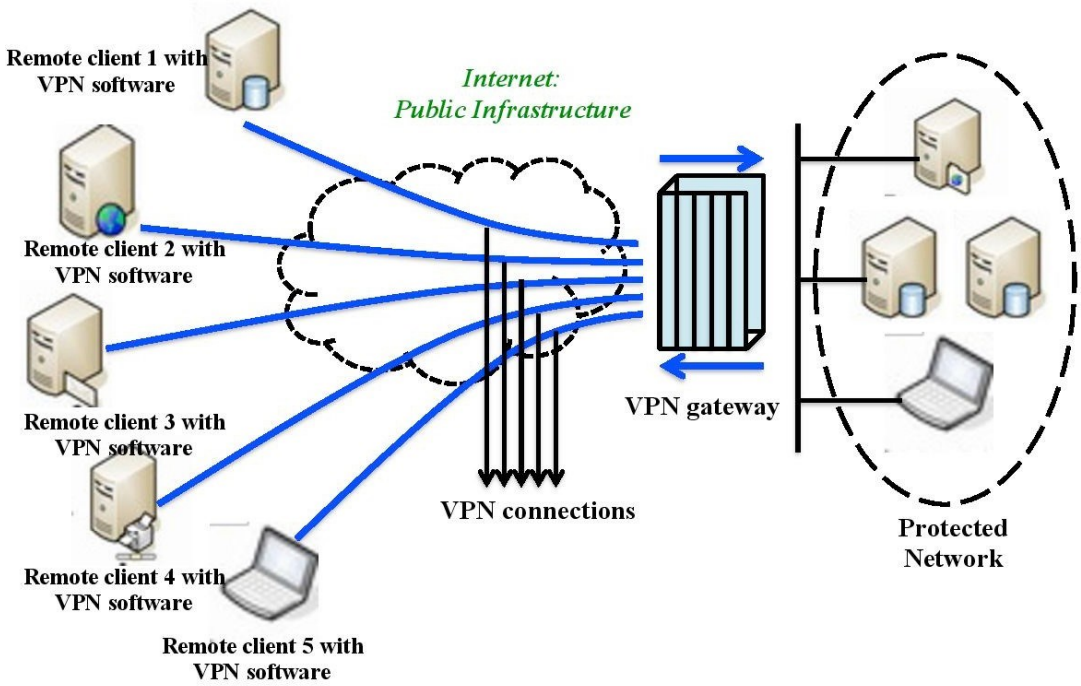
3.3.1 Site-to-site VPNs

In Site-to-site VPNs the hosts/clients/users operating across the VPN tunnel do not require separate installation of VPN client software on each, sending or receiving of TCP/IP traffic is enabled across the VPN gateways. The gateway at one end is responsible for encapsulating, encrypting and authenticating outbound traffic, sending it to the peer VPN gateway at the other end across the public infrastructure to the target site. The VPN peer at the other end, detaches the IP header, decrypts the data and forwards the data packets to the target host in its private network.
The most commonly deployed secure protocol used in setting up site-to-site VPNs is IPSec protocol [23]. VPNs are largely deployed using IPSec protocol because of its ability to enhance productivity and communication thus increasing network flexibility.

Advantage: Site-to-site VPNs offer greater scalability and flexibility because only thegateway VPN needs to support IPSec functionality and hence the installation and management costs across deployed gateways is minimal. Also it offloads the processing overhead from individual systems to the gateway router thus freeing up memory consumption and processing speed.

Disadvantage: However, the processing overheads managed by the gateway routers increaseCPU utilization thus degrading user performance in terms of communication speed.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024



REMOTE ACCESS VPN ARCHITECTURE

Figure 3: Remote Access VPN architecture

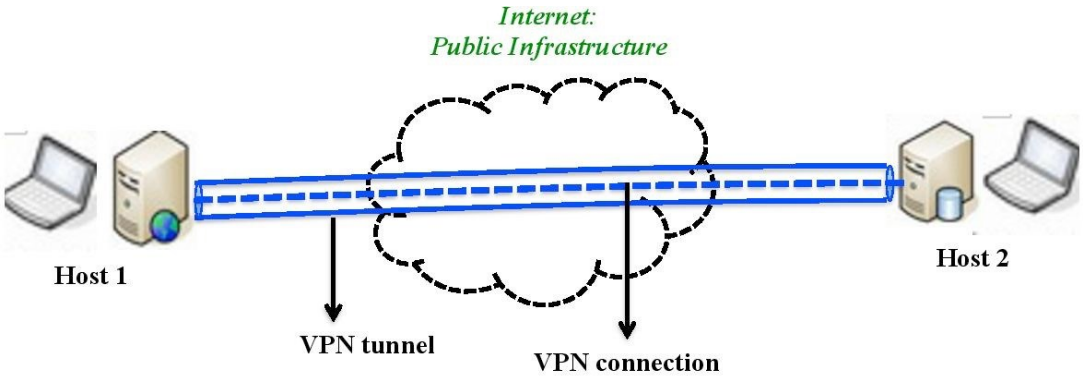
3.3.2 Remote Access VPNs

Remote Access VPNs, every host must have VPN client software. Whenever the host tries to send traffic to the protected network, the VPN client software encapsulates and encrypts the data before sending it over the public infrastructure to the target VPN gateway. Upon reception, the VPN gateway behaves in the same way as the site-to-site peer decrypting and detaching of the IP header before forwarding it to its private subnet.
Remote access VPN protocols are more varied. The Point-to-Point tunneling protocol (PPPTP), layer 2 tunneling protocol (L2TP), SSL/TLS, IPSec are all used to deliver Remote access VPNs.

Advantage: Remote access VPN has its advantages of enhancing productivity, providing secure communication, reducing costs and increasing flexibility of VPNs [28].

Disadvantage: One drawback in these VPNs is that all these approaches require VPN client software to be installed on each remote client and the target VPN gateway that supports the same protocol and extensions for remote access.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024



HOST-TO-HOST VPN ARCHITECTURE

Figure 4: Host-to-host VPN architecture

3.3.3 Host-to-Host VPNs

In host-to-host configurations as shown in Figure 4, a VPN tunnel is establishedbetween two hosts that want to communicate securely without relying on gateways.

Advantage: The main advantage of this approach is that the security is end-to-end.
Disadvantage: The disadvantage is that these VPNs require VPN software to be installed oneach host connected to the VPN.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

4. METHODOLOGY

This chapter describes several aspects related to the cloud-based, VPN test-bed, implementedas part of this work:
Classified into following sub-sections:

- Theoretical approach of IPSec VPN mechanism
- Architectural Framework
  FIWARE: OpenStack CLIs
- Experimental Test-Bed
  StrongSwan
- Route-based configurations
- Software for performance metrics

3.4 Theoretical approach of IPSec VPN mechanism

The establishment of a site-to-site IPSec tunnel can be divided into five steps [20]:

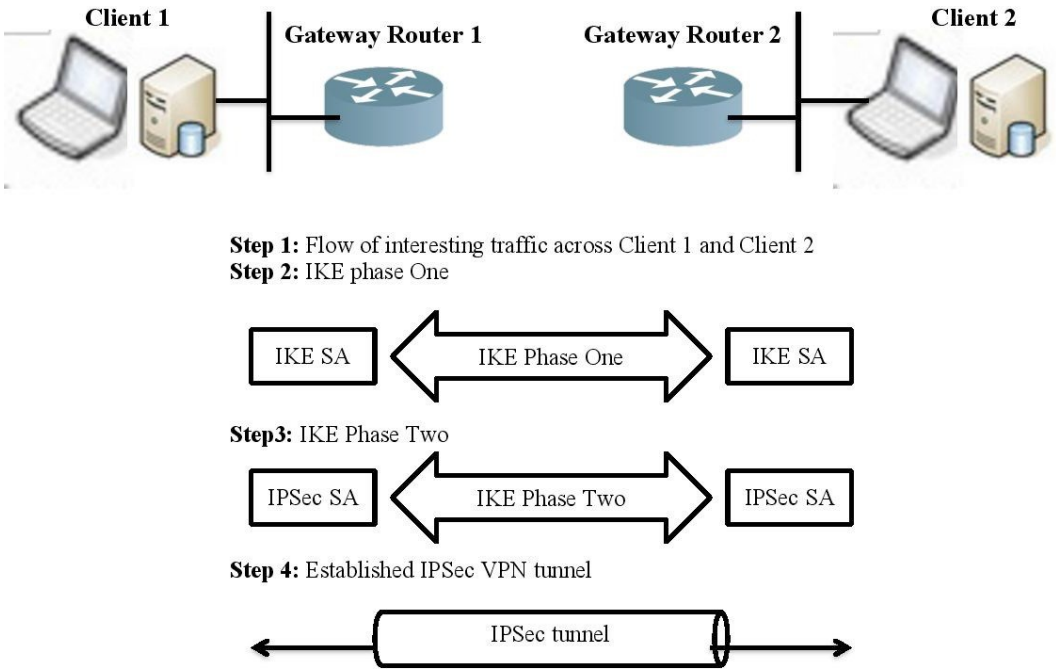


Figure 5: IPSec VPN Working

Step 1: Flow of interesting traffic over the Internet
Determining what type of interesting traffic, protected traffic, is to be sent across the gateways is an important part of building a VPN. The static routes implemented direct traffic going towards the remote end of a tunnel to the local VPN gateway. These routes allow movement of particular traffic through the tunnel to be encrypted and the rest is sent over the unprotected Internet. When traffic to be encrypted is generated or moves
across the clients, the VPN gateways initiate the next step of negotiating the IKE phase one exchange.

Step 2: IKE Phase One - To create IKE Security Association, SA.
Phase 1: The main purpose of IKE phase one is to authenticate IPSec peers and set up secure tunnel across the network to enable IKE exchanges. This phase enables communication across the two VPN gateways, negotiating of new keys and checking on non-responsive devices along with the management variables being transmitted acrossthe IKE SA.
The goals of IKE phase one are as follows:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

- To protect and authenticate the identities of IPSec peers
- Negotiating an IKE SA security policy between the VPN peers to protect theIKE exchange.
- Performs an authenticated Diffie-Hellman exchange with the end result ofhaving to match shared secret keys.
- Set up a secure channel to negotiate IPSec phase two parameters.

Working: IKE phase one creates and authenticates the IPSec peers with the help of policy sets. A policy set defines the policies to secure the channel session, router authentication policies, encryption algorithm used, hashing algorithm used and the key lifetime. It also performs an authenticated Diffie-Hellman exchange resulting in the sharing of secret keys. These policies are agreed upon across the two ends and asuccessful tunnel is establishes if there exist matching parameters. IKE SA is established by negotiation of parameters and thus a bi-directional security association with a secure channel is set-up.

Step 3: IKE phase two – To create IPSec Security Association, SA.
Phase 2: After the successful negotiation of IKE SAs, IKE phase two concentrates onthe negotiation of IPSec SAs to build a secure channel across peers.
The goals of IKE phase two are as follows:

- Negotiate IPSec SA parameters already protected by IKE SAs
- Establishment of IPSec security associations
- Periodically renegotiate IPSec SAs to ensure data security

Working: Phase 2 requires a transform set, placed inside another logical construct and given a name like IPSec profile. This set defines how the end user data is made secure bymatching IPSec profiles or matching transform sets between the routers. If there exist matching security parameters, two security associations are established. One ISAKMP SA is established and two IPSec SAs are established. ISAKMP SA is bi-directional and each IPSec SA is unidirectional. Hence an outbound SA exists to manage traffic from a node 1 to a node 2, and an inbound SA for traffic coming from node 2 to node 1 is required as well. Hence outbound SA exists to route traffic from router 1 to router 2, and an inbound SA for traffic coming from router 2 to router 1. Hence for one VPN tunnel there exists three SAs. One being for management, second for outbound data and the other for inbound data. Each SA is associated with Security Parameter Index, SPI, whichis a 32-bit serial number.
If the data transmitted across the tunnel is sniffed using a packet analyzer tool called Wireshark, IP and ESP packets are observed at layer 3. The SPI is used to indicatethe SA on the receiving node. The SPI may be the same on the inbound and outbound traffic. The SPI is just a number that the receiver uses to lookup the SA for this traffic and applies the correct policies.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

The major difference between IKEv1 and IKEv2 is the number of messages exchanged. IKEv1 functions in two phases: Phase1 (Main mode – 6 messages or Aggressive mode – 3 messages) and Phase 2 (Quick mode – 3 messages).
IKEv2 has no defined phases but makes use of four different messages: IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA and INFORMATIONAL.
A detailed description on the working of IKE v1 and v2 can be studied in [29].
Step 4: Established IPSec channel
After IKE phase two is established, information is exchanged through the IPSec tunnel. Data is encrypted and decrypted across the gateway VPNs as mentioned in the IPSec SA.

Step5: Tunnel Termination
IPSec VPN security associations terminate through deletion or by timing out. A specific security association faces time out when the number of seconds mentioned has elapsed. New SAs can also be established before the existing SAs terminate to continue the flow of traffic uninterrupted.

3.5 Architectural Framework

The framework is divided into sections covering the following topics

3.5.1 FIWARE
3.5.2 FIWARE Lab
3.5.3 OpenStack CLI

4.2.1 FIWARE

FIWARE [30] is a new infrastructure to create services and applications on the Internetto serve the needs of developers in multiple-domains.
As proposed by EU and European Companies, under the FI-PPP program the objectives [31] of FIWARE are as follows:

- To help the development and implementation of new applications and services
- Provide a set of APIs for rapid application development across numerous areas
- To facilitate reuse of resources and introduce standards

Out of the many general-purpose functions available through a set of well-defined APIs, FIWARE Generic Enablers (GE), the functions provided for Security [31] and Cloud Hosting [31] are of significance in this paper.

4.2.2 FIWARE Lab

FIWARE Lab is a working instance of FIWARE available for experimentation providedby FIWARE Generic Enablers deployed as a service either globally or as private instance.
Detailed information on various steps to be followed and parameters defined to launch,deploy and manage VM instances have been referred to in the Appendix D.

4.2.3 OpenStack CLI

Openstack is an open-source cloud computing software platform utilized by users todeploy it is an Infrastructre-as-a-service.

Few of its distinctive features include:

- Provision of horizontal scalability to deploy and launch millions of VMs and billionof stored objects over the distributed architecture [32].
- Compatibility and flexibility in supporting most virtualization solutions such as KVM, Xen etc [32].

Following are the main components of OpenStack which provide the under mentioned services [33]:

- **Nova** – It is also known as the OpenStack compute service, which is responsible for the provision of virtual servers based on the demand and also facilitates cloud resource management through its APIs. The API simplifies the orchestration, launching and controlling of VMs.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

- Glance – It is an OpenStack image service facilitating a lookup and recovering of virtual instances images. The API provides services for registering and discovering VM images along with managing server image libraries.

- Neutron – It is an OpenStack networking service. Neutron service allows users to create and manage various frameworks such as Intrusion detection systems, VPNs and so on and provides potential for managing DHCP, static IPs and VLANs.

- Swift – It is an OpenStack object storage service facilitating users to store and retrieve documents.

- Cinder – It is an OpenStack block storage service which when used along with swiftcan be used to back up large amount of VM volumes.

- Keystone – It is an OpenStack service that facilitated token and authentication, catalog and policy management. It is also responsible for user authentication and granting authentication tokens.

FIWARE provides advanced OpenStack-based cloud hosting capabilitites and a rich library of GE offering a number of added-value functions offered as a *'Service'* [30]. Each OpenStack project has a command-line client to run simple commands for create andmanage cloud resources and automated tasks through simple scripts. Detailed procedure for launching VMs is .

OpenStack Parameters

Following are the parameters essential for launching and deployment a VM:

- Image: Depending on the *type*, *container* and *disk formats*, required images or snapshots can be launched.
- Flavor: Depending on *Virtual CPUs, Memory* and *User Disk*, *tiny*, *small*, *medium*, *large* and *xlarge* flavors are selected depeing on user requirements.
- User data: Files in the metadata service that cloud-aware application in the guest instance can access.
  User_data_two_nics.txt – Launching with 2 NICs
  User_data_one_nic.txt – Launching with 1 NIC.

The *customization script* was composed to enable the gateway routers to be set-up with two NICs default being 1 NIC. Reference to the customization script can be found in the Appendix E.

- Key pair: Keypairs are SSH credentials injected into images when they are launched. Creating a keypair registers the public key and downloads the private key in the form of a *.pem* file. A keypair with desired name is created and following the pop up windows downloads the private key.
- Security group: Security groups are set of *IP filter rules* applied to an instance's networking.
- Meta region: Region where the VM is required to be launched based on user requirements.

Detailed descriptions for deploying VMs through OpenStack CLIs are as follows:

Step 1: Install OpenStack CLI utils on Ubuntu

```
sudo apt-get install python-dev python-pip
```

Step 2: Install the nova and neutron client for Compute and Networking APIs with pip.

```
sudo pip install python-novaclient sudo pip install python-neutronclient
```

Step 3: openrc files are manually created and sourced depending on the number of tenants tobe accessed. Content included in the files can be referred from Appendix B.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

Step 4: List of available flavors, images, security groups, keypairs, and networks can be viewed by executing the following commands

nova flavor-list
nova image-list
nova secgroup-list –all-tenantsnova
keypair-list
nova network-list

Step 5: Launch an instance from an image
nova boot VPN1 --image Ubuntu14.04init --flavor 2 --security-groups=default
--nic net-id=<VPN1 ID>,v4-fixed-ip=10.1.1.12 --nic net-id=<client ID>,
v4-fixed-ip=192.168.1.13 --key-name=Karlskrona2 --user-data user_data_two_nics.txt
--meta region=Karlskrona2

The vpn ID and client ID are the IDs of the network displayed from the nova network-list.

3.6 Experimental Test-Bed

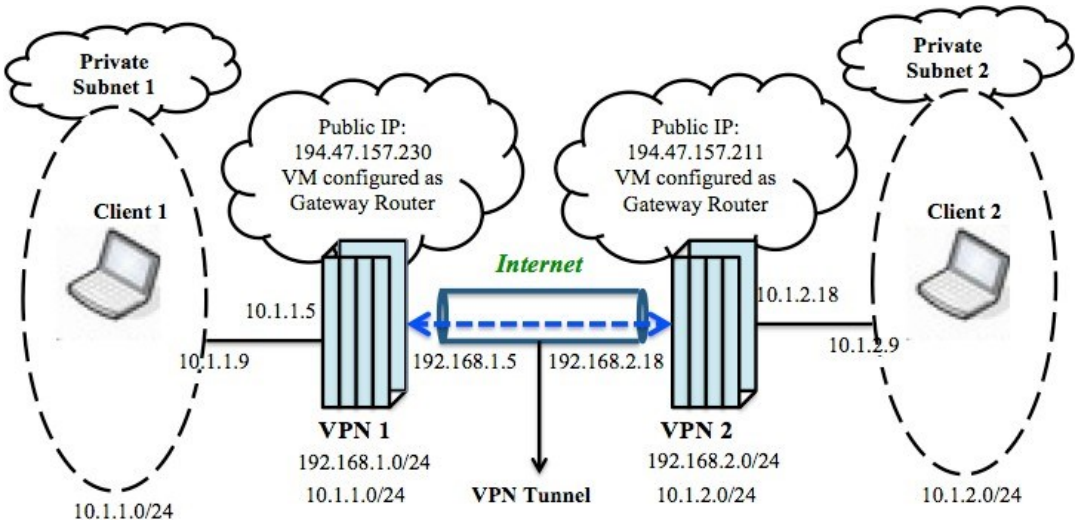


Figure 6: VPN Architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

The main objective of this research is the establishment of a cloud-based IPSec VPN tunnel configured across geographically different locations. For this purpose, a cloud platform such as FIWARE provides the required infrastructure, security and monitoring mechanisms to instantiate the experimental framework. Two tenants are operated with different subnets behind the gateway routers with reference to the steps mentioned in the Appendix A.

Tenant 1 operates a site containing virtualized gateway router, *VPN1* with an associated floating IP from the 194.47.157.0/24 subnet. VPN1 has two interfaces: oneconnected to the internal network 192.168.1.0/24 and another connected to protected network 10.1.1.0/24. The floating IP is paired with the IP address from the internal network in order to allow the VM to communicate over the Internet through the NAT layer operated by OpenStack. Similarly another tenant is set up in a geographically different location. The site at the secondary location contains the virtualized VPN2 gateway router with a floatingIP also from the 194.47.157.0/24 subnet. VPN2 has one network interface connected to the internal network192.168.2.0/24 and another one connected to the protected network 10.1.2.0/24. When a tunnel is established between the two VPN gateways the VM in the twoprotected networks will be able to exchange data. The IP configuration of the VMs operated in the two sites is shown in Figure 7 and 8.

Figure 7: Tenant 1 configuration

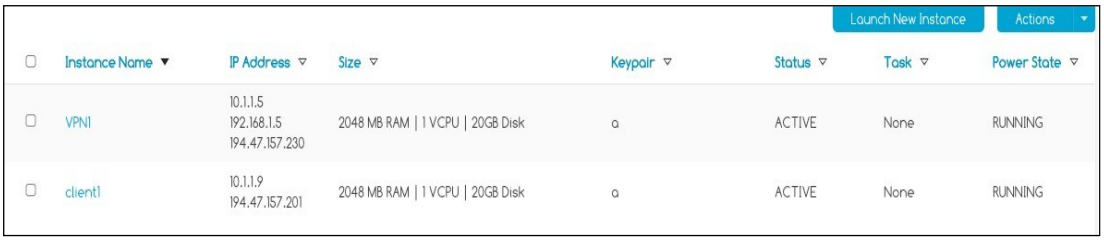


Figure 8: Tenant 2 configuration

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

4.3.1 StrongSwan

StrongSwan [34] is one of the most prominent open source IPSec-VPN based solution implemented across cross-platforms. The main motivation behind the selection ofstrongSwan over other IPSec implementation software's like OpenSwan etc., is its wide adaptability to different Linux distributions, implementation of both IKEv1 and IKEv2 key exchange protocols, extendibility to many plugins and enhanced documentation reports. strongSwan IKEv2 is inherently multi-threaded while OpenSwan is single-threaded thus enabling the former to handle thousands of concurrent IPSec tunnels on VPN gateways. strongSwan also provides better support for authentication, security mechanisms and is modular compared to the monolithic behavior of OpenSwan.
To accomplish the tunnel architecture across peer-to-peer gateways, strongSwan software is installed inside two VMs that act as VPN gateways as explained in the previous section. StrongSwan is a complete IPSec solution providing encryption and authentication to servers and clients [34].

Few of its advantages [34] are listed below:

- StrongSwan supports IKEv2 interoperability one of its efficient advantages over others.
- Numerous tunnels handling capacity of strongSwan IKEv2 which is inherently multi-threaded is superior to OpenSwan, which is single-threaded.
- StrongSwan is modular and offers distinct plugins enhancing its functionality.

The features and functionalities of IKE and IPSec can be referred from chapter 3.
StrongSwan [34] is a keying daemon, using the IKEv1 or IKEv2 protocols to establish SAs across the peers. The goal of IKE is to provide strong authentication of both peers and deriveunique cryptographic session keys. These IKE sessions denoted by *IKE_SA* [34] provide the means to exchange configuration information and to negotiate IPSec SAs, denoted by *CHILD_SAs*. These IPSec SAs define the interested traffic to be sent across the tunnel and how the data is encrypted and authenticated. The *CHILD_SA* [34] consists of two elements, the actual IPSec SA describing the encryption, hashing algorithm and keys required to encrypt and authenticate the traffic and the policies to define which traffic shall use such an SA. The policies work both ways, i.e., only traffic matching an inbound policy will be decrypted at the other end.
The experimental set-up for achieving site-to-site VPN connectivity across gateway routers, VPN1 and VPN2, are configured can be referred to from Appendix A.
As mentioned in the section *IPSec VPN associations*, the functionalities, operation and performance clearly depict transparency to applications, ability to secure real-time traffic andIPSec VPNs competence to highly secure site-to-site connectivity. *StrongSwan* is one of the most projecting implementations of IPSec VPNs on Linux platforms in comparison to the already existing software of OpenVPN, OpenSwan etc.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

StrongSwan parameters

- IP address: The left and right IP addresses are assigned with the VPN1's private IP and VPN2 peer's public IP respectively.

VPN1	VPN2
Left=192.168.1.5	*Left=192.168.2.18*
Right=194.47.157.211	*Right=194.47.157.230*

- IDs: *Leftid* and *rightid* are denoted to specify the identity of the left ad rightendpoint.

VPN1	VPN2
Leftid=@sun.strongswan.org	*Leftid=@moon.strongswan.org*
Rightid=@moon.strongswan.org	*Rightid=@sun.strongswan.org*

- Tunnel: *Conn tunnel* denotes the connection of the tunnel with the name *tunnel*, connection established at one end.

- Subnets: The left and right subnets are the private subnets for secure data access.

VPN1	VPN2
Leftsubnet=10.1.1.0/24	*Leftsubnet=10.1.2.0/24*
Righsubnet=10.1.2.0/24	*Rightsubnet=10.1.1.0/24*

- IKE and ESP protocols: The *ike* and *esp* options are used to denote variouscombinations of encryption algorithm and hashing algorithms. Analyses have been performed examining various encryptions and hashing algorithms.
  As a responder of the *tunnel*, both daemons accept the first supported proposal received from the peer.

- Keyingtries: This option can be set to any positive integer, indicating the number of attempts to be made to negotiate a connection.

- Ikelifetime and lifetime: These parameters indicate the period after which thekeying channel of connection and particular instance of a connection i.e., a set of encryption and authentication keys is to be renegotiated respectively.

- Authby: This option denotes the key distribution mechanism used to authenticate the peer-to-peer gateways. *Authby = secret/psk* can be used to denote pre-shared keying.

- Keyexchange: The protocol used for *keyexchange=ikev2* to initialize the connectiondue to ikev2's support and enhanced functionalities.

- Dead peer detection: The *dpdaction*, *dpdtimeout* and *dpddelay* options are specifiedto detect activity

4.3.2 Validation and verification of tunnel authenticity

Detailed description on the communication and tunnel establishment by various parameters is mentioned in [29]. Following commands are executed to validate the establish the tunnel and verify its authenticity:

- sudo ipsec up <name of the tunnel>

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

```
root@vpn1:~# sudo ipsec up tunnel
establishing CHILD_SA tunnel
generating CREATE_CHILD_SA request 2 [ SA No KE TSi TSr ]
sending packet: from 192.168.1.5[4500] to 194.47.157.211[4500]
received packet: from 194.47.157.211[4500] to 192.168.1.5[4500]
parsed CREATE_CHILD_SA response 2 [ SA No KE TSi TSr ]
```

Figure 9: Security associations across tenant 1 and 2

```
root@v2:~# sudo ipsec up tunnel
establishing CHILD_SA tunnel
generating CREATE_CHILD_SA request 2 [ SA No KE TSi TSr ]
sending packet: from 192.168.2.18[4500] to 194.47.157.230[4500]
received packet: from 194.47.157.230[4500] to 192.168.2.18[4500]
parsed CREATE_CHILD_SA response 2 [ SA No KE TSi TSr ]
```

Figure 10: Security associations across tenant 2 and 1

Figures 9 and 10 display the Security Association built across both the peer gateways where *No* denotes Nonce, *KE* stands for Key Exchange, *TSi* and *TSr* for Traffic Selector Initiator and Traffic Selector Responder respectively. Sending a *CREATE_CHILD_SA* request creates a *CHILD_SA*. The initiating peer sends SA request in *SA* paylod, a nonce,a Diffie-Hellman value in *KE* payload and the proposed traffic selectors in the *TSi* and *TSr* payloads. Now, the responding peer accepts the *SA* in the *SA* payload, a nonce value in KE payload and traffic selectors in the *TSi* and *TSr* payloads.

- sudo ipsec statusall

```
Connections:
      tunnel:  192.168.1.5...194.47.157.211, dpddelay=30s
      tunnel:   local:  [vpn1.strongswan.org] uses pre-shared key authentication
      tunnel:   remote: [vpn2.strongswan.org] uses any authentication
      tunnel:   child:  10.1.1.0/24 === 10.1.2.0/24 , dpdaction=clear
Security Associations:
      tunnel[2]: ESTABLISHED 61 seconds ago, 192.168.1.5[vpn1.strongswan.org]...
194.47.157.211[vpn2.strongswan.org]
      tunnel[2]: IKE SPIs: 1f3d99a049c001ad_i a42ae7c11e116ffc_r*, pre-shared ke
y reauthentication in 43 minutes
      tunnel[2]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
      tunnel{3}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c306fbb2_i cfc5d5e5_o
      tunnel{3}:  3DES_CBC/HMAC_MD5_96, 0 bytes_i, 0 bytes_o, rekeying in 7 hour
s
      tunnel{3}:   10.1.1.0/24 === 10.1.2.0/24
      tunnel{4}:  INSTALLED, TUNNEL, ESP in UDP SPIs: c0dda63a_i c118d5ff_o
      tunnel{4}:  3DES_CBC/HMAC_MD5_96, 0 bytes_i, 0 bytes_o, rekeying in 7 hour
s
      tunnel{4}:   10.1.1.0/24 === 10.1.2.0/24
```

Figure 11: Validation of established tunnel across the two sites

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

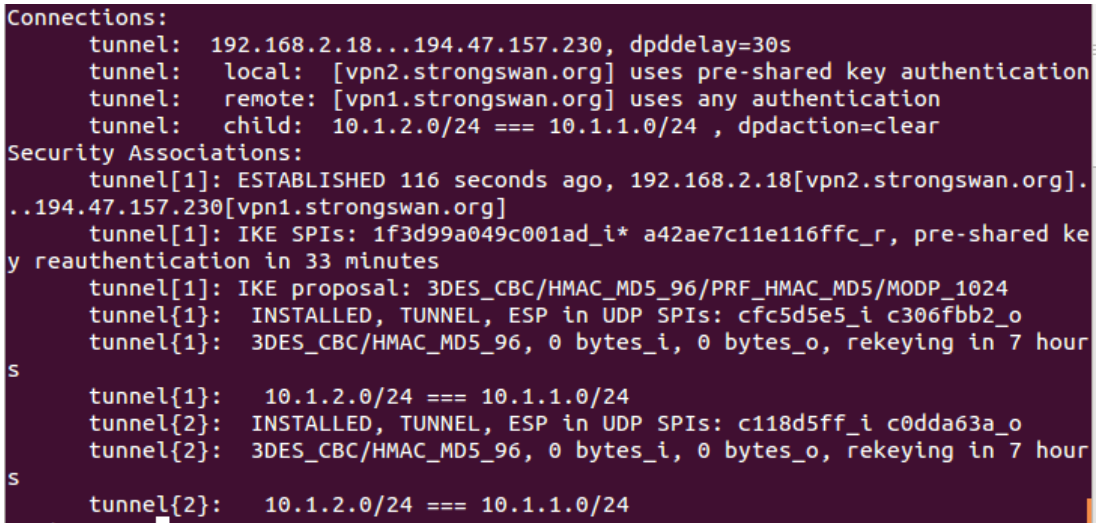


Figure 12: Validation of established tunnel across the two sites

Figures 11 and 12 display the time since the tunnel was created, the key authentication mechanism used, the protocol used for encryption and mode in which IPSec was operated. *10.1.1.0/24 === 10.1.2.0/24* and *10.1.2.0/24 ===10.1.1.0/24* denoted the private networks secured across the two ends.
IP forwarding is enabled across the VPN peers ensures traffic is routed through theVPN tunnel, when the interesting traffic surpasses the client and reaches the gateway router.

4.3.3 Route-based configurations

To route the client traffic from different subnets through respective VPN gateways,static routes are configured across the client systems. These routes force the client traffic to surpass through the VPN interfaces to ensure all private traffic flows through the tunnel and is secure through encryption at both ends.

Across subnet 1,
up route add –net 10.1.2.0 netmask 255.255.255.0 gw 10.1.1.5

Across subnet 2,
up route add –net 10.1.1.0 netmask 255.255.255.0 gw 10.1.2.18

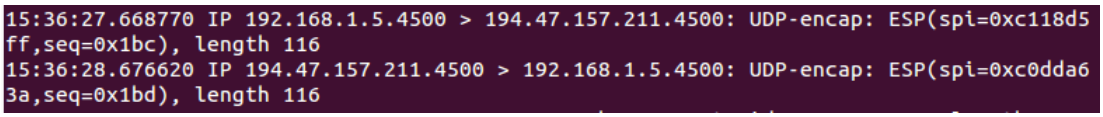


Figure 13: ESP traffic to ensure packets flow through the tunnel at Tenant 1

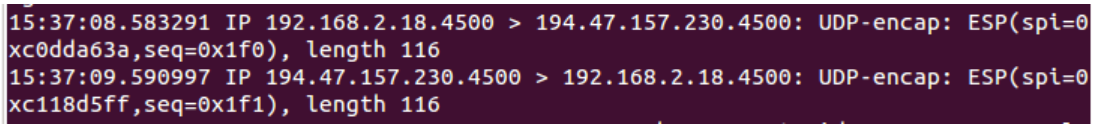


Figure 14: ESP traffic to ensure packets flow through the tunnel at Tenant 2

Figures 13 and 14 observes ESP packets, at the peer gatewys by using *tcpdump* depicting traffic being routed through the tunnel. The client source and destination address are encrypted and encapsulated, and the new header displays the source and destination addresses of VPN peers thus protecting and securing client traffic from attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

4.3.4 Software for Performance Metrics

Iperf [35] is a network-testing tool/network performance measurement tool with the capability of creating TCP and UDP streams and measures the throughput of the network carrying them. Written in C language it enables the user to set various parameters required for testing the network. It has client and server functionality to measure the throughputacross the two ends, either unidirectional or bi-directional. *Iperf* reports throughput, jitter andpacket loss. TCP and UDP analysis have been calculated with the *iperf* tool and resulting statistics are deduced.

4 RESULTS

This section involves a detailed study on different combinations of encryption and hashing algorithms considered in the experimental procedure to determine the cryptographic, metric and overhead analysis involved in each case. The different encryption algorithms considered are AES526, AES128 and 3DES; the hashing algorithms considered are SHA256 and MD5. The parameters considered are TCP throughput, UDP throughput, and jitter and packet loss. These parameters are measured for different MTU values to understand the impact of packet size on overheads. Comparative analyses on tunneled and non-tunneled traffic are computed to determine the overhead of encryption in a virtualized environment. All the measurements are plotted with 95% confidence intervals.

4.2 Brief description of Algorithms

5.1.1 Advanced Encryption Standard

AES comprises of variable length ciphers including 128-bit and 256-bit key length ciphers. Each cipher encrypts and decrypts data in blocks of 128 and 256 bits using 128- bit and 256-bit cryptographic keys respectively. Due to its high computational complexity, AES is considered to be of high speed and reliability assuming the approximate cipher cracking time to be 149 trillion years [36] [37].

5.1.2 Triple Data Encryption Standard

With the expanding computer processing power, the 56-bit DES algorithm is considered inadequate to keep data secure for a longer period. It is referred to as *3DES,* since it encrypts the data three times each with different keys increasing the productivity of the same algorithm. Each has a 64-bit key length, summing it to a 192-bit symmetric key algorithm. Despite its slow speed, the approximate cracking time of this algorithm is considered to be 4.6 billion years with current technology [36] [37].

5.1.3 Secure Hash Algorithm

SHA2 [38, p. 2] stands for 2nd version of Secure Hash Algorithm designed to overcome the vulnerabilities imposed by the 1st version, SHA1. SHA2 is a cryptographic hash function with a digest length of 256 bits. In comparison to SHA1, SHA2 is considered stronger and longer hashes are generated for data security.

5.1.4 Message Digest Algorithm

MD5 stands for Message Digest Algorithm 5, which verifies data integrity through the creation of a 128-bit message digest from data input of any length [39, p. 5]. Despite being slower in comparison to MD4, it offers higher assurance of data security.

4.3 Results for TCP traffic

The bandwidth for different combinations of encryption and hashing algorithms are reviewed for different MTU sizes. Each measurement has been iterated 30 times with a time period of 10 seconds each. The TCP congestion control algorithm used for this research is the default *CUBIC.* This algorithm is considered to be a less aggressive variant of BIC that is Binary Increase Congestion Control. In TCP, different packet sizeswith MTU 1500, 1000, 500 and 250 are considered. Graphs are plotted at differentMTUs against their achieved throughputs for different algorithms. Non-tunneled traffic indicates the traffic measured for plaintext data and the tunnel traffic using differentencryption algorithms for cipher text data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

5.2.1 Throughput analysis

In tunnel mode, IPSec VPNs are built and managed across end-to-end gateways.As mentioned in the previous sections, tunnel mode protects any internal routing information by encrypting the IP header of the entire packet, followed by the encapsulation of a new IP header to the original header.

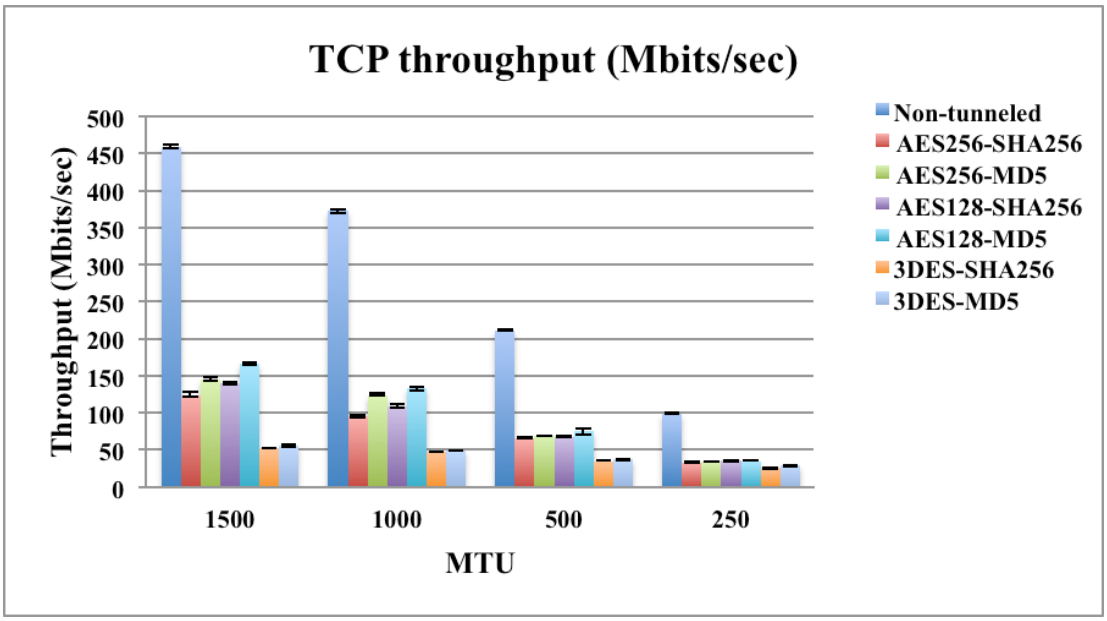


Figure 15: TCP throughput at different MTUs

The overheads due to encryption lower the network throughput to a great extent. Variation in throughout between tunneled and non-tunneled traffic is clearlydepicted in the graph.

Comparison among different encryption and hashing algorithms are evaluated, superior performance is exhibited by AES128-MD5 in terms of throughput. The reason being, in comparison to the other hashing algorithm, SHA256, MD5 produces128-bit output and SHA256 produces 256-bit output that further brings an additional overhead resulting in performance degradation. Also MD5 is considered to be less CPU intensive in comparison to SHA family [40]. Though, SHA is considered to be more secure, MD5 operates faster and hence its performance. In comparison to the other encryption algorithms, 3DES was initially designed for hardware models and hence its low efficiency in software implementations, where AES was designed both for software and hardware implementations and hence its superior performance. In comparison to AES128 and AES256, depending on the cryptographic key length, the longer more is the overhead introduces [41].

Few of the drawbacks of 3DES functionality are the usage of weaker and shorter keys in comparison to AES, repetitive encryption keys used and the longer time duration compared to AES [42]. All these factors enhance the performance efficiency of AES128-MD5. Hence AES128-MD5 performs the best, followed by AES256-MD5 and AES128-SHA256.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

4.4 Results for UDP traffic

To ensure good link quality, packet loss of the network is maintained below 1% [35]. UDP throughput and jitter are calculated between different combinations of encryption and hashing algorithms for different packet sizes of 1500, 1000, 500 and 250.

5.3.1 Throughput analysis

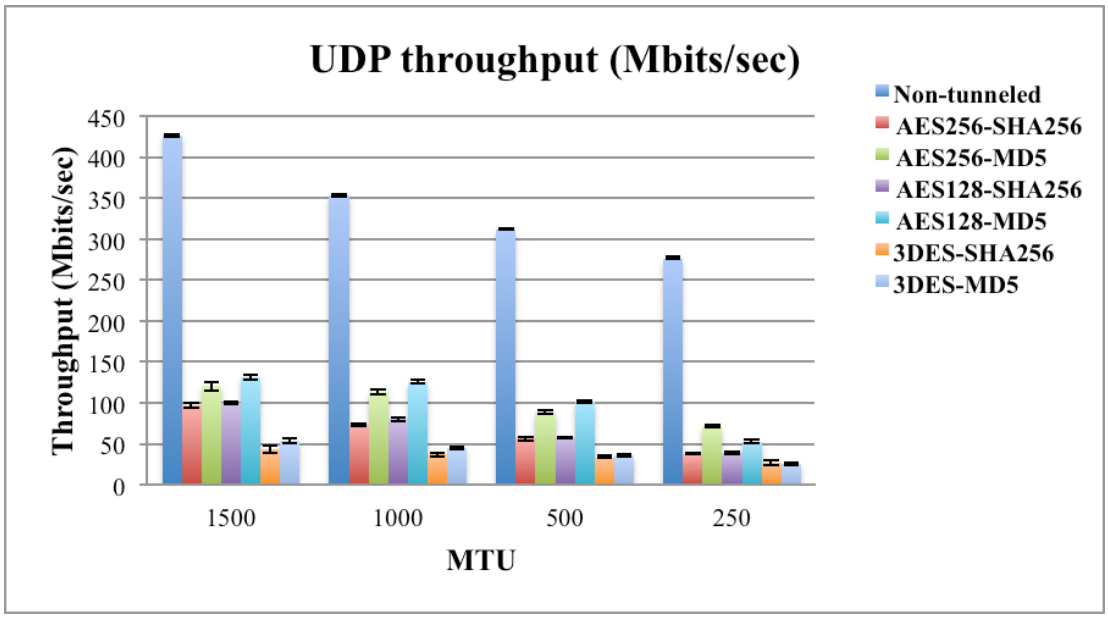


Figure 16: UDP throughput at different MTUs

Similar algorithmic performance is observed by UDP packets, where AES128-MD5 performs the best followed by AES256-MD5 and AES128-SHA256. Reasons being the same due to the deteriorative performance by SHA in comparison to MD5 and the superiority of AES over 3DES.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

5.3.2 Jitter analysis

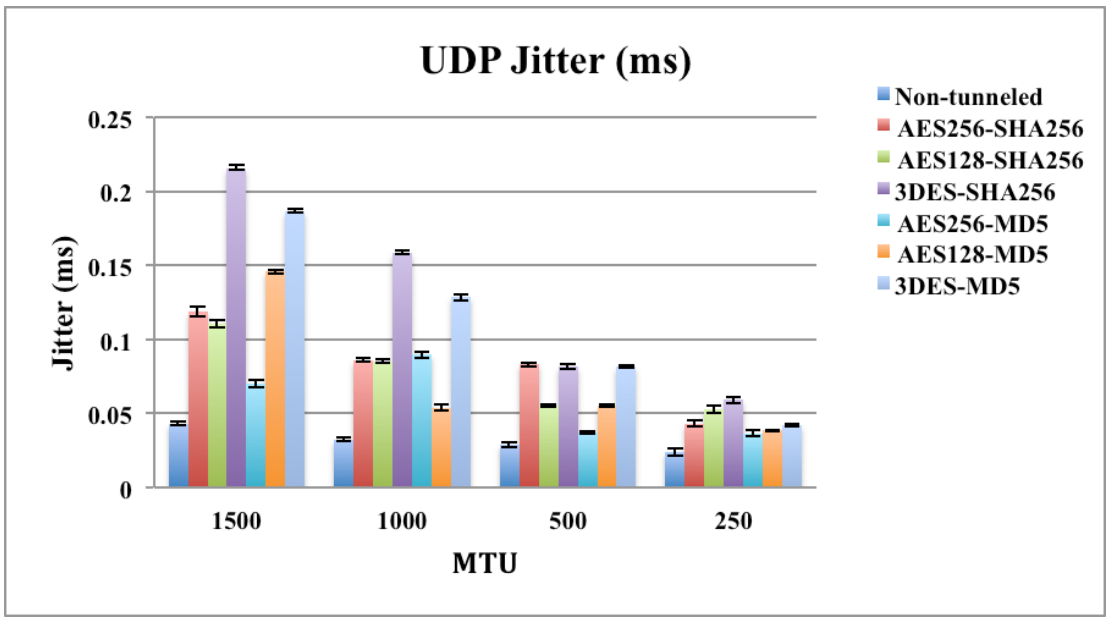


Figure 17: UDP Jitter at different MTUs

Jitter is considered among different combinations of encryption and hashing algorithms with different packet sizes. The jitter for tunneled traffic is observed to be more than in non-tunneled/plaintext traffic, due to additional overhead introduced for data encryption. Extra cryptographic overheads increase network complexity thus increasing jitterin the network. DES is observed to exhibit the maximum delay in comparison to the other combinations, because of similar reasons involving hardware compatibility, weak and slowerkeys and longer time period.

4.5 Results for resource allocation

4.5.1 VM provisioning latency

According to the NFV Service Quality Metrics document published by ETSI [43], VM provisioning latency is the time elapsed between a VM provisioning request being presented and the corresponding response being returned. The average value required forVM resource allocation is measured and evaluated below along with 95% confidence interval.

Average	23.4 sec ≈ 23 seconds
Half-length 95 % Confidence Interval	0.72 ≈ 1

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

4.5.2 VM Failure Ratio

According to the NFV Service Quality Metrics document by ETSI [43], VM Failure Rate is the ratio of VM instances delivered to the VNF customer. It is defined as the ratio of total failed attempts to launch VM to the total number of successful attempts. Over the 30 iterations calculated, the numbers of successful attempts recorded of VM instantiation were 30 and the failed attempts were recorded to be zero. Thus the average value for VM Failure Rate is measured to be ***zero.***

Average	0

4.5.3 Service operational time

According to the NFV Service Quality Metrics document by ETSI [43], VM service start up time/operational time is the time elapsed for VM provisioning and time required for setting up the VPN tunnel. The values measured for setting up the VPN tunnel were recoded to be 2 seconds. Thus the total operational time including VM start up time and VPN servicestart up time was measured to be 23.4+2.4 ≈ 25.8 seconds. The average value of VPNservice start up time has been tabulated below.

Average	2.4 ≈ 2 seconds
Half-length 95% Confidence Interval	0.18

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

5 ANALYSIS AND DISCUSSIONS

5.2 Requirements to offer VPN as a VNF

A comparative study on different architectures reviewed in the previous sections give a detailed analysis on the different designs stating the pros and cons of each, enabling cloud users to determine the best suited. Comparative analysis on the different modes of operation including the tunnel and transport mode has also been studied, stating each of its advantages and disadvantages for better efficiency and suitability. Various key distribution mechanisms have also been reviewed for enhancing security mechanism in the cloud, concentrating on pre-shared keys for this research to avoid IPSec complexities [15].

Being a VNF, VPNaaS could be included in complex service chains that can be automatically managed and configured to provide sophisticated virtualized services. Among the high level requirements stated by the NFV document proposed by ETSI [44], including portability, performance, elasticity, resilience, security, service continuity and so on, following are the requirements identified to provision VPN as an VNF:

5.2.1 Portability

According to the ETSI document, when talking about software-based implementations of VPNs in virtualized environment on general-purpose hardware, thecapability of shifting, configuring and executing of VPN based VNFs across different vendors but standard hypervisor environments, standard experimental infrastructures such asdeployment in XIFI are to be attained [44].

In this research, portability of VPN solution is achieved by executing the same procedural model on various architectures. It has been achieved across the FIWARE federated cloud as well as on VMware hypervisor. Thus achieving portability across various hypervisors and experimental platforms considered to be an important aspect in Virtualizing Virtual Private Networks.

5.2.2 Service stability and continuity

In addition to portability as mentioned in the NFV virtualization requirements,establishing and ensuring service stability and continuity is yet another important factor for virtualizing VPNs, specifically when re-locating or re-configuring the software-based implementations in the virtualized environment [44].

The maximum and minimum values of attainable throughput, recorded packet loss ratio, latency variations are specified in this research as the key performance indicators to ensure service continuity across the network. Packet loss is maintained less than 1%, to ensure network stability [45].

5.2.3 Security

In this report, the security issue is governed through the implementation of various encryption and hashing algorithms. Since security is of prime importance when deploying VPNs as a Virtualized Network Function, requirements are to be made to ensure data integrity; confidentiality and authenticity are not compromised.

5.2.4 Operational requirements

The responsibility of instantiation, allocation, re-allocation and termination of VPN resources are important operational requirements that virtualized environments provide to cloud tenants according to the ETSI norms [44].

The resource allocation metrics like VM provisioning latency, VM Failure Ratio andVPN service operational time are measured and analyzed in the current research. These measurements exhibit the speed and reliability of resource allocation across different geographical locations. Thus it is necessary to accommodate similar VMs that can be run on the same hypervisor platform with minimal performance degradation operating on the same compute nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

5.3 Measuring metrics

Since dealing with VPNs introduces additional IP headers and complex processing of cryptographic operations, the overhead introduced during data transmission has been studied. Measuring the link throughput gives details on network performance, which can be further studied and analyzed with the number of packets lost during transmission and with the delay encountered. Network throughput is defined as the rate at which data is transmitted over a communication channel. In addition to providing secure data over dedicated links, reliability of the established connection channel is also equally important for simulating a directconnection. The reliability of the network depends largely on the throughput of data in the connection. Hence to ensure secure and reliable transfer of data, throughput is taken as one for important parametric analyses.

Jitter is defined as the inter-arrival time variation between packets to their destination. Good transmission network record jitter values between 1 to 5 milliseconds [46]. Low jitter values help in maintaining the inter-packet delay introduced by the source, which is ofutmost importance when dealing with small sized packets.

Packet loss takes place when packets travelling across a channel fail to reach their destination network. To ensure good link quality, packet loss of the network is maintained below 1% in this research [45]. Higher the loss of packets in the network, greater will be the TCP segment retransmissions, ultimately affecting available network bandwidth [35].

VM resource allocation metrics involving VM start up time, VM service start up time and VM Failure Ratio are measured and evaluated to determine reliability and speed of orchestration management.

6.2.1 Cryptographic Analysis

Taking into account the different combinations of encryption and hashing algorithms, it is observed that AES128-MD5 outperforms in all the cases **Figure 15** and **Figure 16** thisis due to design of AES for efficient implementation in both hardware and software exhibiting satisfactory efficiency, stronger cryptographic keys of 256-bit key length in comparison to repetitive weak and slower keys and longer time duration for 3DES encryption. Also the key schedule for AES128 is considered stronger to AES256 when considering resistance to related-key attacks since the longer the source master key, the morecontrol over the sub keys is required thus weakening security in related key attack models [47].

3DES was designed for efficient hardware implementation, but its inferior performance with software, nearly 3 times less when compared to software implementations was outperformed by AES [48]. MD5 is considered less CPU intensive in comparison to SHA family and hence exhibited superior performance to SHA [40]. Though, SHA isconsidered to be more secure, MD5 operates faster and hence its performance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

6.2.2 Metric Analysis

Since VPNs simulate a confidential connection, throughput through a VPN tunnel is often affected by the overheads and complex processing algorithms used. An appropriate method to compute maximum network throughput is by minimizing delay introduced by keeping the packet loss below 1%.

During TCP packet analysis, from the results evaluated it is observed that the best throughout was exhibited by AES128-MD5 followed by AES256-MD5 and AES128- SHA256. The worst performed were 3DES-SHA256 and 3DES-MD5. Reasons being inefficient implementation of software, weaker key performance and longer time period of 3DES in comparison to AES.

To maintain good link quality, the packet loss is retained less than 1% throughout the calculative analysis [45]. UDP packets observed similar cryptographic performance to TCP. Similarly, AES128-MD5 showed best throughput and 3DES-SHA256 exhibited lowest performance.

Jitter is considered for different combinations of encryption and hashing algorithms with different packet sizes. The jitter for tunnel traffic is observed to be higher than in non- tunneled or plaintext traffic, due to additional overhead introduced while encrypting data. Extra cryptographic overheads in addition to extra IPSec headers increase network complexity thus increasing jitter in the network. DES is observed to exhibit the maximum jitter in comparison to the other combinations, because of software incompatibilities.

6.2.3 Overhead analysis

Throughput and Jitter are calculated for different MTU sizes. In TCP, it is observed that as the as the MTU increased, the throughput across the network also increased

[12] [13] [14]. Emphasis was laid on providing reliable and secure transmission of data and hence despite the variable packet sizes, the packet loss of the network was maintained below1%. Similar performance was observed in TCP and UDP, throughput of the network in UDP exhibited further superiority when packet loss in the network was compromised and allowed to exceed 1%. But to ensure good link quality, packet loss was reduced to less than 1%. The overhead introduced due to tunneled traffic comprised of the additional IPSec header and encryption complexity degrades network performance for both TCP and UDP traffic.

6.2.4 Resource allocation analysis

- Reliability

The VM Failure Rate is observed to be zero, for all iterations calculated indicating resource allocation reliability. The VM Failure ratio evaluated to 0 ensures optimal reliabilityof delivering the VM instance with VPN requirements to a VNF customer.

- Speed

VM start up time and VPN service start up time are measured and analyzed to estimate the speed of resource allocation, launching and VPN deployment. Maximum attainable time required for offering VPN as a VNF are also evaluated and recorded to be 2 seconds which is the time required for setting up a secure VPN connection for confidential data transmission.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

6 CONCLUSIONS AND FUTURE WORK

6.2 Summary

The goal of the thesis was to provide VPNaaS prototype for the cloud. The objectives achieved are a detailed study involving the various architectural implementations of VPNs and a detailed study regarding the various key distribution mechanisms for security enhancement. Also a Linux based cloud platform for facilitating communication across different elements, configuration and modeling of an open source based IPSec VPN solution with *strongSwan* has been achieved. Followed by the performance evaluation of various encryption algorithms to estimate the overheads introduced.

Among the various implementations studied, site-to-site architecture has been adopted ensuring network security, routing, encapsulation and encryption to be performed by the gateway routers devoid of the clients/users participation by using IPSec in tunnel mode. The IKEv2 interoperability and modular feature of *strongSwan* draws efficiency over other available software. Low infrastructure costs and ease to deploy a new network adds to its scalability and flexibility features. Among the various key distribution techniques studied in chapter 3, pre-shred keys are used in this implementation to avoid complex configurations.

VPN architecture was modeled and designed with FIWARE federated cloud lab and OpenStack CLIs. One of the primary elements to be calculated in offering VPN prototype to the cloud is the effect on performance introduced by the model. Despite, having heavy amounts of overhead introduced, a good reason for this model's adoption would be to enhance and account for cloud characteristics and ensure secure data transmission across the peer elements.

Among the different combinations of encryption and hashing algorithms used, AES128-MD5 performed the best in comparison to 3DES-SHA256 that produced the least throughput. VM resource allocation metrics also evaluated the maximum time durations required for launching and establishment of VPN service in the virtualized environment. These metrics describe the speed and reliability factors necessary for launching and orchestration of cloud services.

An important part of this research is the identified requirements in offering VPN as a Virtualized Network Function. Achieving portability across standard hypervisors and experimental platforms, ensuring service stability and continuity by analyzing the attainable throughout and jitter values, keeping the packet loss minimal are important factors for managing VPN services across virtualized servers. Also the main aim of building VPNs is toensure security in the cloud for secure and confidential communication. Various operational evaluations are conduced to investigate the speed and reliability of VM resource allocation, deployment and management in the cloud environment. The low VPN service time enables the model to be utilized for secure telephonic conversations, wherein the time taken to set upthe tunnel before communication is only around 2 seconds.

Linking answers to the research questions mentioned have been briefly summed up. The various architectures including site-to-site, host-to-host and remote access VPNs suitable for implementing virtual VPNs have been studied and stated along with each advantages and disadvantages. Also the various key distribution mechanisms including pre- shared keys and digital certificates have been studied and a clear description of each hasbeen mentioned. The design and modeling of an IPSec VPN solution on a cloud platform has

been adopted for implementation in this thesis further answering the RQ based on the modeling of a cloud based VPN solution. Also the performance impacts on the built model are evaluated with both TCP and UDP traffic. Network throughput, jitter and packet loss are measured for different encryption and hashing algorithms thus studying the impact of thebest algorithmic combination on each of the evaluated metric and also stating secure cryptographic combinations for confidential transfer of information, thus answering thefourth RQ.

6.3 Future work

6.3.1 OpenStack - VPNaaS

In OpenStack networking, VPNaaS is a neutron-extension also based on IPSec based VPN implementation [49]. The feature set also involves the implementation of IKE with PSK authentication. Since similar work involving authentication has been performed in this research,

future work could revolve around a comparative analysis of the current research and OpenStack based VPNaaS.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

6.3.2 Caching to reduce overheads

The performance analysis conducted by the authors of [23], deduced caching to bean effective strategy to reduce the IKE overheads introduced. With reference to the cryptographically secure cache resumption protocol introduced in [23], the choice of cachingstrategy and duration depends on the detected vulnerabilities in any environment. The same could be implemented in the cloud model, to reduce overheads and gain better VPN performance.

6.3.3 Detailed protocol overhead analysis

Detail analysis and evaluation can be performed on overheads introduced by ESPand IKE protocols to determine the exact percentage of overheads induced into the network and its causes. Similar Site-to-Site VPNs architectures can be modeled, using other key distribution mechanisms such as Digital Certificates and Public key encryption to evaluate and compare different architectures. Performance metrics such as CPU utilization, power consumption considered important service quality metrics for cloud-based users and VNF customers can also be calculated.

6.3.4 Security improvements with IDS

Providing data confidentiality and authentication to sensitive information are ofutmost importance to cloud-based users, compromising on security during data traversing isa major setback. In addition to the encryption provided, VPN systems can be installed with host-based intrusion detection systems that monitors and analyses the internals of a system along with network packets. Algorithms can be designed to detect specific intrusion attacks and counter measuresdesigned to mitigate them. Encrypting of data can be made stronger, usage of digital signatures and certificates and usage of bandwidth and throughput throttling techniques can be adopted for proper validating and filtering of output.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

7 REFERENCES

[1] J. Y. Lee, J. W. Lee, D. W. Cheun, and S. D. Kim, "A quality model forevaluating software-as-a-service in cloud computing," in Software Engineering Research, Management and Applications, 2009. SERA'09. 7th ACIS International Conference on, 2009, pp. 261–266.

[2] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," Commun. Mag. IEEE, vol. 53, no.2, pp. 90–97, 2015.

[3] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1113–1122, 2011.

[4] M. Forsman, A. Glad, L. Lundberg, and D. Ilie, "Algorithms for automated live migration of virtual machines," J. Syst. Softw., vol. 101, pp. 110–126, 2015.

[5] A. A. Alsaheel and A. S. Almogren, "A Powerful IPSec Multi-Tunnels Architecture," J. Adv. Comput. Netw., vol. 2, no. 4, 2014.

[6] W.-H. Liao and S.-C. Su, "A Dynamic VPN Architecture for Private Cloud Computing," in Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on, 2011, pp. 409–414.

[7] D. Shinder, "Comparing VPN Options," WindowSecurity.com. [Online]. Available:http://www.windowsecurity.com/articles- tutorials/firewalls_and_VPN/VPN-Options.html. [Accessed: 03-Sep-2015].

[8] "Advantages and Disadvantages of IPsec - Best," VPN Services Reviews. .

[9] L. Andersson and T. Madsen, "Provider provisioned virtual private network(VPN) terminology," 2005.

[10] "9 top threats to cloud computing security," InfoWorld, 25-Feb-2013. [Online]. Available: http://www.infoworld.com/article/2613560/cloud-security/cloud- security-9-top-threats-to-cloud-computing-security.html. [Accessed: 03-Sep- 2015].

[11] "Data Protection In The Cloud Era," Network Computing. [Online]. Available: http://www.networkcomputing.com/cloud-computing/data-protection-in-the- cloud-era/240161485. [Accessed: 03-Sep-2015].

[12] B. Hoekstra, D. Musulin, and J. J. Keijser, "Comparing TCP performance of tunneled and non-tunneled traffic using OpenVPN," Univ. Van Amst. Syst. Netw. Eng. Amst., pp. 2010–2011, 2011.

[13] S. S. Kolahi, Y. R. Cao, and H. Chen, "Bandwidth-IPSec security trade-off in IPv4 and IPv6 in Windows 7 environment," in Future Generation Communication Technology (FGCT), 2013 Second International Conference on, 2013, pp. 148–152.

[14] S. S. Kolahi, Y. Cao, and H. Chen, "Evaluation of IPv6 with IPSec in IEEE 802.11 n wireless LAN using Fedora 15 operating system," in Computers and Communications (ISCC), 2013 IEEE Symposium on, 2013, pp. 000203–000206.

[15] S. Srivatsan, M. L. Johnson, and S. M. Bellovin, "Simple-VPN: Simple IPsec Configuration," 2010.

[16] M. H. M. Zaharuddin, R. A. Rahman, and M. Kassim, "Technical comparison analysis of encryption algorithm on site-to-site IPSec VPN," in Computer Applications and Industrial Electronics (ICCAIE), 2010 InternationalConference on, 2010, pp. 641–645.

[17] C. J. C. Pena and J. Evans, "Performance evaluation of software virtual private networks (VPN)," in 25th Annual IEEE Conference on Local Computer Networks, 2000. LCN 2000. Proceedings, 2000, pp. 522–523.

[18] A. Andelic, M. Koprivica, and B. Bozilovic, "Experimental performance evaluation of VPN implemented with strongSwan client and Cisco IOS IPSec gateway," in Telecommunications Forum (TELFOR), 2011 19th, 2011, pp. 162– 165.

[19] C. Shue, Y. Shin, M. Gupta, and J. Y. Choi, "Analysis of IPSec overheads for VPN servers," in Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNPWorkshop on, 2005, pp. 25–30.

[20] N. Doraswamy and D. Harkins, IPSec: The New Security Standard for theInternet, Intranets, and Virtual Private Networks. Prentice Hall Professional, 2003.

[21]S. Frankel, K. Kent, R. Lewkowski, A. D. Orebaugh, R. W. Ritchey, and S. R. Sharma, "Guide to IPsec VPNs," NIST Spec. Publ., pp. 800–77, 2005.

[22] D. Bendell, Configuring SonicWALL Firewalls. Syngress, 2006.

[23] C. Shue, M. Gupta, S. A. Myers, and others, "Ipsec: Performance analysis and enhancements," in Communications, 2007. ICC'07. IEEE International Conference on, 2007, pp. 1527–1532.

[24] S. Kent, "IP encapsulating security payload (ESP)," 2005.

[25] "ESP header description - Google Search." [Online]. Available: https://www.google.se/webhp?sourceid=chrome- instant&ion=1&espv=2&ie=UTF-8#q=ESP+header+description. [Accessed: 02-Sep-2015].

[26] K. Seo and S. Kent, "Security Architecture for the Internet Protocol." [Online]. Available: https://tools.ietf.org/html/rfc4301. [Accessed: 03-Apr-2015].

[27] R. Hunt, "PKI and digital certification infrastructure," in Networks, 2001. Proceedings. Ninth IEEE International Conference on, 2001, pp. 234–239. [28]"Remote-Access VPNs: Business Productivity, Deployment, and Security Considerations,"Cisco.[Online].Available:http://cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation- firewalls/prod_white_paper0900aecd804fb79a.html. [Accessed: 20-Aug-2015].

[29] C. Kaufman, "Internet key exchange (IKEv2) protocol," 2005.

[30] M. Reyes, "FI-WARE DEVELOPERS PORTAL » FIWARE." [Online]. Available: https://www.fiware.org/fi-ware-developers-portal/. [Accessed: 19-Aug-2015].

[31] "Introduction to FI-WARE," 09:28:00 UTC.

[32] O. Sefraoui, M. Aissaoui, and M. Eleuldj, "OpenStack: toward an open-source solution for cloud computing," Int. J. Comput. Appl., vol. 55, no. 3, pp. 38–42, 2012.

[33] T. Rosado and J. Bernardino, "An Overview of Openstack Architecture," in Proceedings of the 18th International Database Engineering & ApplicationsSymposium, New York, NY, USA, 2014, pp. 366–367.

[34] A. Steffen, the OpenSource IPsec-based VPN Solution: StrongSwan. .

[35] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, and K. Gibbs, "Iperf tutorial," May, 2005.

[36] C. GUO and others, "MEASUREMENT OF VPN PENFORMANCE BETWEEN DIFFERENT DEVICES," 2013.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

[37] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in Information and communication technologies, 2005. ICICT 2005.First international conference on, 2005, pp. 84–89.

[38] "SHA-2," Wikipedia, the free encyclopedia. 30-Jul-2015.

[39] "What is MD5? - Definition from WhatIs.com," SearchSecurity. [Online]. Available: http://searchsecurity.techtarget.com/definition/MD5. [Accessed: 16-Aug-2015].

[40] "cryptography - Is calculating an MD5 hash less CPU intensive than SHA family functions?StackOverflow."[Online].Available:http://stackoverflow.com/question s/2722943/is-calculating-an-md5-hash-less-cpu-intensive-than-sha-family- functions. [Accessed: 04-Sep-2015].

[41] W. Stallings, Network security essentials: applications and standards. PearsonEducation India, 2007.

[42] H. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, Y. Al-Nabhani, and others, "New comparative study between DES, 3DES and AES within nine factors," ArXiv Prepr. ArXiv10034085, 2010.

[43] Dr. Julien Maisonneuve, Alcatel-Lucent, "Network Functions Virtualisation (NFV); Service Quality Metrics." .

[44] Susana Sabater, Vodafone Group PLC, "Network Functions Virtualisation (NFV); Virtualization Requirements." .

[45] "http://openmaniak.com/iperf.php." .

[46] "http://www.certusdigital.com/index.php?option=com_content&view=article&id =58:why-is-jitter-important&catid=34:questions-a-answers&Itemid=29." .

[47] "encryption - Is AES-256 weaker than 192 and 128 bit versions? – Cryptography StackExchange."[Online].Available:http://crypto.stackexchange.com/questions/5 118/is-aes-256-weaker-than-192-and-128-bit-versions. [Accessed: 05-Sep-2015].

[48] "Comparison of DES, Triple DES, AES, blowfish encryption for data - Stack Overflow."[Online].Available:http://stackoverflow.com/questions/5554526/com parison-of-des-triple-des-aes-blowfish- encryption-for-data. [Accessed: 16-Aug-2015].

[49] "VPNaaS_IPsecSpecific_blueprint," Google Docs. [Online]. Available: https://docs.google.com/document/d/1Jphcvnn7PKxqFEFFZQ1_PYkEx5J4aO5J 5Q74R_PwgV8/edit?usp=embed_facebook. [Accessed: 04-Oct-2015].

[50] "Fiware cloud capabilities_and_setting_up_your_environment," 07:21:47 UTC. [51]R. Fisli, "Secure Corporate Communications over VPN-Based WANs," Masters Thesis Comput. Sci. Sch. Comput. Sci. Eng. R. Inst. Technol. Swed., 2005.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

APPENDIX A

VPN GATEWAY CONFIGURATIONS

(i) VPN CONFIGURATIONS IN TENANT 1

In /etc/ipsec.conf the following configuration changes are to be added:

config setup
conn %default
conn tunnel
left=192.168.1.5
leftsubnet=10.1.1.0/24
leftid=@vpn1.strongswan.org
right=194.47.157.211
rightsubnet=10.1.2.0/24
rightid=@vpn2.strongswan.org
ike=aes256-sha2_256-modp1024!
esp=aes256-sha2_256!
keyingtries=0
ikelifetime=1h
lifetime=8h
dpddelay=30
dpdtimeout=120
dpdaction=clear
authby=secret
auto=start
keyexchange=ikev2
type=tunnel

In /etc/ipsec.secrets the below line is added:

@vpn1.strongswan.org @vpn2.strongswan.org : PSK
0sv+NkxY9LLZvwj4qCC2o/gGrWDF2d21jL
@vpn1.strongswan.org %any : PSK 0x45a30759df97dc26a15b88ff
@vpn2.strongswan.org : PSK "prototypetestingpassword"
: PSK “prototypetestingpassword” 192.168.1.2 :
PSK "prototypetestingpassword"

(ii) VPN CONFIGURATIONS IN TENANT 2

config setup
conn %default
conn tunnel
left=192.168.2.18
leftsubnet=10.2.2.0/24
leftid=@vpn2.strongswan.org
leftfirewall=yes right=194.47.157.230
rightsubnet=10.1.1.0/24
rightid=@vpn1.strongswan.org
rightnexthop=%defaultroute
ike=aes256-sha2_256-modp1024!

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

esp=aes256-sha2_256-modp1024!
keyingtries=0
ikelifetime=1h
lifetime=8h
dpddelay=30
dpdtimeout=120
dpdaction=clear
authby=secret
auto=start
keyexchange=ikev2
type=tunnel

In /etc/ipsec.secrets the below line is added:

@vpn1.strongswan.org @vpn2.strongswan.org : PSK
0sv+NkxY9LLZvwj4qCC2o/gGrWDF2d21jL

APPENDIX B

OPENSTACK CLIs

(i) OPENRC FILE FOR TENANT 1

export OS_TENANT_ID= 00000000000000000000000000012913
export OS_USERNAME=vpn1@gmail.comexport
OS_PASSWORD=<secret>
export OS_AUTH_URL=http://cloud.lab.fi-ware.org:4730/v2.0/ export
OS_REGION_NAME=Karlskrona2
export OS_AUTH_STRATEGY=keystone

(ii) OPENRC FILE FOR TENANT 2

export OS_TENANT_ID=72bbf279cb3444739bef26c47a7bac1e export
OS_USERNAME=vpn2@yahoo.co.in
export OS_PASSWORD=<secret>
export OS_AUTH_URL=http://cloud.lab.fi-ware.org:4730/v2.0/ export
OS_REGION_NAME=Karlskrona2
export OS_AUTH_STRATEGY=keystone

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

APPENDIX C

MTU	Non-tunneled	AES256-SHA256	AES256-MD5	AES128-SHA256	AES128-MD5	3DES-SHA256	3DES-MD5
1500	459	124.2	144.9	139.75	165.65	52.185	56.22
1000	372	95.34	124.2	108.465	133.05	47.615	49.71
500	211	66.165	68.88	67.335	74.775	34.89	37.18
250	99	33.24	34.63	35.26	34.87	25.19	28.755

Figure C1: TCP Throughput at different MTUs (Mbits/sec)

MTU	Non-tunneled	AES256-SHA256	AES256-MD5	AES128-SHA256	AES128-MD5	3DES-SHA256	3DES-MD5
1500	425.65	96.54	120.27	100.47	130.87	42.96	54.33
1000	352.6	73.8	113.43	80.56	125.58	36.86	45.59
500	311.8	56.65	88.16	58.09	101.83	33.76	35.43
250	276.4	38.18	71.38	39.19	52.63	26.88	25.86

Figure C2: UDP Throughput at different MTUs (Mbits/sec)Maximum 1% packet loss tolerated

MTU	Non-tunneled	AES256-SHA256	AES128-SHA256	3DES-SHA256	AES256-MD5	AES128-MD5	3DES-MD5
1500	0.043	0.118666667	0.110333333	0.215666667	0.07	0.145666667	0.186666667
1000	0.0322	0.086	0.085333333	0.158333333	0.089666667	0.054	0.128333333
500	0.029	0.083	0.055333333	0.081666667	0.037	0.055333333	0.082
250	0.0364	0.043	0.052666667	0.059	0.024	0.040333333	0.042

Figure C3: UDP Jitter at different MTUs (ms)Maximum 1% packet loss tolerated

MTU	Non-tunneled	AES256-SHA256	AES128-SHA256	3DES-SHA256	AES256-MD5	AES128-MD5	3DES-MD5
1500	0.16	0.72	0.81	0.003	0.42	0.016	0.60
1000	0.44	0.71	0.90	0.016	0.52	0.19	0.23
500	0.023	0.45	0.41	0.23	0.80	0.42	0.28
250	0.87	0.91	0.17	0.29	0.90	0.79	0.19

Figure C4: Packet loss below 1%

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

APPENDIX D

WORKING WITH FIWARE LAB

Cloud end users can provision, manage, deploy and launch their resources through the FIWARE Dashboard or though the OpenStack command-line clients.

FIWARE Dashboard

Following are the steps for launching an instance and editing security groups for accessing ofVM in the cloud:

Step 1: Create an account in lab.fiware.org

Enter the username and password credentials to login into the account, if not *sign up* with anew account.

Step 2: Enter into the cloud-hosting portal

On entering the right credentials, the page is redirected to the cloud portal where, to the left margin blueprint, compute and storage are managed.

Step 3: Create keypair (private key)

Keypairs are SSH credentials injected into images when they are launched []. Creating a keypair registers the public key and downloads the private key in the form of a *.pem* file.

A keypair with desired name is created and following the pop up windows downloads theprivate key.

Step 4: Deploy instance

Next under the compute section, the *images* of the required VM under the *Name* tab and *type* can be selected and launched under the *action* tab.

The Launch Instances pop up is controlled with 4 steps [50].

- **Details:** Under this tab, the Instance Name, Flavor and Instance Count arespecified. The selected details are dynamically shown under the Project Quotas section.
- **Access and Security:** Control Access is issued to the instances with the help of keypairs, security groups etc. The keypair created in Step 3 is selected from the dropdown, default security groups chosen or new security groups added accordingly.
- **Post-Creation:** The customization script generated corresponds to User Data in other systems. Depending on the options available in the script, the launched instance is customizable.
- **Summary:** The Instance Name, Image, Flavor, Instance Count, Keypair and Security Group so selected are verified before launching the instance.

Step 5: Allocate floating IP address (public IP)

After the instance is launched, to communicate across the Internet, floating IP address i.e., public IPs are allocated from a pool of floating IPs.

Step 6: Edit Security Groups

A security group with port 22 is to be included in Security Group tab to access via SSH. Similarly, other ports are also to be opened depending on the accessibility requirements of VM by editing the security group rules.

For instance,

Port -1 is to allow all ICMP traffic

Port 80 is to allow HTTP

Port 4500 for enabling the VM to listen to IKE messages

Port 5001 is to enable iperf, network-testing tool, to send and acknowledge TCP and UDP packets.

Completion of the above steps launches the Virtual Machine accessible through SSH via port22.

For instance through SSH, ssh –i keypair.pem root@<floating IP of VM>

Enterprises benefit from VPN in reducing the cost, increasing the stability, and increasingthe productivity, without impairing the security [51].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

APPENDIX E

OPENSTACK CLIs CUSTOMIZATION SCRIPTS

Customization Script for Launching VM with one NIC

```
#cloud-config #
# This script automatically permorm some needed actions for the VM configuration#
You can modify it, but be careful not to change network configuration. write_files:
- encoding: b64
content: |

YXV0byBsbyAKaWZhY2UgbG8gaW5ldCBsb29wYmFjawogYXV0byBldGgwIAogaWZh
Y2UgZXRoMCAgaW5ldCBkaGNwCg==
path:  /etc/network/interfaces

-   content: |
    DEVICE="eth0"
    NM_CONTROLLED="yes"
    ONBOOT="yes"
    BOOTPROTO="dhcp"
    TYPE="Ethernet"
    path: /etc/sysconfig/network-scripts/ifcfg-eth0
    permissions: '460'

    bootcmd:
 - ifdown eth0
 - ifup eth0

# Start DEM monitoring
runcmd:

- curl  -L  -s  -k  https://xifisvn.esl.eng.it/wp3/software/DEM_Adapter/install.sh  |  bash

# FIWARE Support
fiware-support:
sshkey: <ssh-key string>

gpgkey: |
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

<GPG key-string>
-----END PGP PUBLIC KEY BLOCK-----
```

Customization Script for Launching VM with two NICs

```
#cloud-config #
# This script automatically permorm some needed actions for the VM configuration
```

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

```
# You can modify it, but be careful not to change network configuration.
write_files:
- encoding:
b64content: |

YXV0byBsbyAKaWZhY2UgbG8gaW5ldCBsb29wYmFjawogYXV0byBldGggwIAogaWZh
Y2UgZXRoMCAgaW5ldCBkaGNwCiBhdXRvIGV0aDEgICBpZmFjZSBldGgxICBpbmV0
IGRoY3AK
path:  /etc/network/interfaces

-   content: |
    DEVICE="eth0"
    NM_CONTROLLED="yes"
    ONBOOT="yes"
    BOOTPROTO="dhcp"
    TYPE="Ethernet"
    path: /etc/sysconfig/network-scripts/ifcfg-eth0
    permissions: '460'
-   content: |
    DEVICE="eth1"
    NM_CONTROLLED="yes"
    ONBOOT="yes"
    BOOTPROTO="dhcp"
    TYPE="Ethernet"
    path: /etc/sysconfig/network-scripts/ifcfg-eth1
    permissions: '460'

    bootcmd:
  - ifdown eth0
  - ifup eth0
  - ifdown  eth1
  - ifup eth1

    # Start DEM
    monitoringruncmd:
  - curl  -L  -s  -k  https://xifisvn.esl.eng.it/wp3/software/DEM_Adapter/install.sh  |  bash

    # FIWARE
    Supportfiware-
    support:
    sshkey: <ssh-key string>

    gpgkey: |
    -----BEGIN PGP PUBLIC KEY BLOCK-----
    Version: GnuPG v1

    <GPG key-string>

    -----END PGP PUBLIC KEY BLOCK-----
```