e-ISSN: 3027-0650
Vol. 2, Issue 1, pp 271-281, November 6 -9, 2024

Implementing Advanced Security Measures in Asterisk-Driven VoIP Networks

Washima Tuleun
Independent Researcher, Makurdi Benue State, 08069189725, {gwtjen@gmail.com}

Abstract - Voice over Internet Protocol (VoIP) is a rapidly advancing technology that facilitates the transmission of voice and audio signals over the Internet or an IP-based network in real-time. This technology has seen a significant rise in demand due to its advantages over traditional circuit-switched telephony, including lower call rates, reduced operational costs, easier management, and enhanced call features. However, the growth in VoIP usage has also increased the potential for various security threats and attacks, jeopardizing the privacy, confidentiality, and integrity of transmitted data. This paper presents the design of an Asterisk-based VoIP system and the implementation of a comprehensive security solution across the VoIP network. The study involves an in-depth analysis of VoIP technology, identifying its vulnerabilities and addressing potential threats. A security framework is proposed and implemented to safeguard the VoIP network. The designed system and security solutions are rigorously tested and evaluated to ensure robustness and effectiveness. The findings highlight critical security measures necessary for protecting VoIP infrastructures and provide a framework for future research and development in securing VoIP networks.

Keywords: Asterisk, Codec, Cybersecurity, IPsec, Malware, Network Security, Phishing, Telecoms, Threats, Telephony, VoIP

1 INTRODUCTION

Voice over Internet Protocol (VoIP) revolutionized telecommunications by enabling voice communication over networks, beginning with VocalTec's first internet softphone in 1995 [1]. Early VoIP faced challenges due to limited bandwidth and poor modem technology [2]. However, broadband improvements enhanced VoIP's Quality of Service (QoS), leading to its widespread adoption and potential to replace traditional PSTN systems [3]. VoIP uses internet broadband to transmit voice over IP networks, reducing communication costs and enabling advanced communication applications like web and video conferencing [4]-[7].

VoIP offers cost savings by avoiding the high tolls of conventional telecommunication lines, and supports rich media services such as voice and video calls [8]-[10]. Its open standards allow integration with backend systems and features like user attributes can move with users globally. However, VoIP's complex service architecture makes designing and troubleshooting challenging, and it depends on power supply, making it vulnerable to outages, unlike PSTN systems with backup power [11]. Security concerns are also significant as VoIP services are more vulnerable compared to PSTN systems. VoIP networks perform more tasks than PSTN, including gateway functions, without requiring all the equipment used in PSTN networks [12].

2 VOIP – Components, Codec, security threats and attacks

The network Component. Includes routers, switches, firewalls, cabling, and PBX [12]. These components must detect, prioritise, and allow VoIP traffic to reach its destination [13] reducing latency. The IP PBX switches calls between VoIP and PSTN users, making it vital to the network [14].

Gateways convert voice calls or signals between packet switched and circuit switched networks in real time [15] and divides gateways into three categories namely:

Media gateways which carries voice signals over IP networks. It detects calls, originates them, and converts analogue to digital voice. **Media gateway controllers** that signal which control, and coordinate the media gateway. [13] Explains that this component's duties include host searching, resource management, phone number translation, and signal functionality. **End-user equipment**; allows network endpoint connectivity. VoIP, soft, and classic phones with audio and video conferencing, instant messaging, and surveillance features may be used by end users [16].

VoIP phones use TCP/IP to communicate with the parent IP network and can be configured manually or using DHCP [17]. Soft phone software can be installed on a PC and used to make calls online [43]

VoIP protocols and codecs – [12] VoIP protocols are categorized into two main categories namely;

Signalling protocols. [18] Defines signalling protocols as those responsible for call setup, monitoring, teardown, and setup negotiation, management, and modifications. These protocols ensure user location, negotiate call sessions, and manage calls. [19] Identified SIP and H.323 as the most commonly used signalling protocols in the VoIP market.

Session Initiation Protocol (SIP) is an application layer signalling protocol primarily used for establishing, modifying, and terminating multimedia sessions between endpoints [20] and [21]. The design philosophy and architecture of the system can be considered to have been derived from the hypertext transfer protocol (HTTP) and the simple mail transfer protocol (SMTP), hence guaranteeing its simplicity [22].

H.323 **-** This protocol establishes a decentralised structure for developing multimedia applications, such as VoIP [44] and facilitates communication between different devices. It is largely utilised for ISDN video conferencing systems and toll pass VoIP applications, as stated by [23]. [24], categorise the H.323 network into the following fundamental components: Endpoints, Gatekeepers that offer signalling services, Multipoint control units that guarantee the accessibility of conferencing services and Gateways. [25].

Media transport protocols. [12] states that media transport protocol controls voice sample encoding, decoding, digitization, and ordering for real-time communication. Media transport protocols, such as real-time and real-time control protocols will be examined here.

The real time protocol is designed to transmit real-time audio or video data over a user data protocol (UDP) [26] however it does not guarantee real-time delivery [18] RTP offers features such as identifying payload type, sequence number, monitoring data transmission, and time sharing. The Real Time Control protocol (RTCP) provides feedback on the quality of service of transmitted data disseminated using real-time protocols. RTCP monitors VoIP issues such latency, delays, and jitters and communicates control information [27].

[28] Defines CODEC as an algorithm that is used to encode and decode voice streams across a network. Encoding is done to enable the voice signal which is Analog to be digitalized and transmitted across the network.

VoIP Codec - At the receiver's end, the signal needs to be decoded, hence its conversion back to Analog stream. The digitization of voice streams is categorized into two processes: sampling and quantization [29]. Common VoIP CODEC used include G.711, G.722, G723.1, G.726 and G.729 [30]

VoIP security threats, attacks, and vulnerabilities - Security of users can be analysed by examining threats, attacks, and vulnerabilities in VoIP networks. [31] And [32] categorized VoIP threats into those against availability, confidentiality, and integrity. Threats against availability disrupt VoIP services, such as denial of service [30]. Examples include call flooding, call hijacking, spoofed messages, and server impersonation [33]

Threats against confidentiality involve stealing caller identities, such as eavesdropping, impersonation, and call pattern tracking [32] and [34] Threats against integrity alter intercepted messages, like call rerouting and media alteration [35] and [11].

Threats against social context involve misrepresenting identities to convey false information [11]. Examples include phishing and spam [35].

Best practices for VoIP security and deployment - A comprehensive security strategy is essential to counter rising VoIP threats. Key practices include:

Network Address Translation (NAT): NAT converts private IP addresses to public ones, concealing internal IPs and adding security [36]. Research by [37] and [13] shows NAT enhances security and addresses IP limitations.

Firewall Deployment: Firewalls, positioned at network boundaries, filter traffic and protect against intruders [13] and [34] Proper deployment prevents unauthorized access [32]. [38] Categorizes firewalls into packet filtering, application-level gateway, and circuit-level gateway.

Virtual Private Network (VPN): VPNs secure data transmission over public networks through encryption [39] and [36] VPN types include site-to-site and remote access [40]. IPSec VPN and SSL VPN provide high levels of security .In conclusion, NAT, firewalls, and VPNs are essential for securing VoIP networks.

Based on the review, it has been narrowed down the Network address translation deployment, firewall deployment and Virtual private network.

3 METHODOLOGY

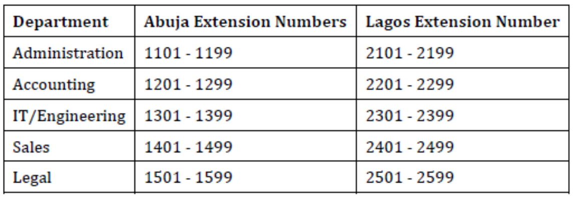
The methodology adopted is based on outlining the technical requirements for carrying out the design and implementation of the network design, the VoIP dial plan and numbering system was also designed, VoIP design methods and the choice of the design tools to be made use of was analysed. In addition, secondary data sources such as research papers, publications, and internet and journal newspapers was used for descriptive sections of the research. Several factors were taken into consideration from the in depth literature review before the implementation design methods was adopted. Factors ranging from the Quality of service issues in Voice over IP networks, security considerations and concerns was analysed in depth and critically.

4 REQUIREMENTS FOR THE VOIP TELEPHONY NETWORK DESIGN.

The requirements of the based design aspect range from Design of an asterisk VoIP based system, Design and integration of a voicemail service system in the Asterisk PBX, Design of a suitable dial plan for the two network site locations and Design and integration of a security solution across the network

Branches with their offices and number of extensions needed - The list of offices and departments in Lagos and Abuja is crucial for designing the dial plan, influencing the choice of the numbering system. During implementation, soft phones were chosen over hard phones due to the limited availability of the latter.
Design of the dial plan and numbering system – [41] stated that dial plan is very important since it handles the inbound and outbound calls in the network through a set of instructions that asterisk have to follow. A four digit dial plan is made use of in the implementation of the project and numbering system. The reason behind this is to give a greater room for expansion of the organisation should the need arise.

Table 1.0: Dial plan table



Department	Abuja Extension Numbers	Lagos Extension Number
Administration	1101 - 1199	2101 - 2199
Accounting	1201 - 1299	2201 - 2299
IT/Engineering	1301 - 1399	2301 - 2399
Sales	1401 - 1499	2401 - 2499
Legal	1501 - 1599	2501 - 2599

Methods and tools used for the design
Asterisk IP PBX; The choice of the asterisk was made since it's an open source, it will be cost effective to deploy, easy to manage, easy access to support as against propriety software, ease of management, little or no complexity in the configuration of the asterisk PBX to include addition features such as auto attendant, voice mail, call conferencing among others..

Session initiation protocol (SIP); this protocol was chosen for its ease of implementation as opposed to other protocols that could also be used for instance the H.323 protocol [34], [21].
IPsec VPN; this offers a strong form of security in the form of encryption, encapsulation of packets and tunnelling during the transmission of data across the network [39]. comparison was made between the IPsec VPN, Secure socket layer (SSL) VPN, firewall deployment and it the adoption of the IPsec VPN was done since its more advantageous and stronger in comparison to the other security methodologies. This is also supported by research done by reputable authors like [42].

Four Digit Dial plan Numbering system; There is room for growth and also because of its scalability as opposed to the three digit numbering system. [43].
Voice mail design; this configuration of the voicemail is achieved by inserting the appropriate settings in the Voicemail.conf file present in the etc/asterisk folder on the asterisk server.

5 SECURITY IMPLEMENTATION ACROSS THE ASTERISK-BASED VOIP NETWORK.

There is the strong need to ensure the security of the VoIP network against unauthorized entry by malicious users. The adoption of the IPsec VPN as against the other security solutions for implementation is based on the numerous advantages it has over others, some of which include but not restricted to;

Encryption and tunnelling allow secure voice packet transmission over the network, enhancing data security and confidentiality. It is also more scalable, flexible and reliable as opposed to the other security solutions. It is cheaper and easier to deploy as opposed to other security solutions and its maintenance and running cost is low
The IPsec site-to-site VPN was chosen for this project due to its ability to maintain confidentiality, site to site security and anonymity. AES encryption was selected for the project. IPsec VPN ensures safe data transit between crypto-enabled peers hence ensuring a secure data transfer between the different peers. IPsec includes two protocols for better security: the Authentication header and Encapsulation Security Protocol (ESP) and the Internet Security Association and Key Management (ISAKMP). To ensure the proper security of the transmitted data, the use of a symmetrical encryption algorithm and the internet key exchange mechanism for safe exchange of keys is recommended.

This security method prevents packet eavesdropping and alteration. Network administrators can modify Hashed Message Authentication codes to enhance setting strength. The IPSec VPN ensures sender-receiver authentication, ESP protocols assure data confidentiality, and AH protocols maintain integrity.

Tools used for design implementation

The design of the VoIP telephony solution was done making use of both soft phones and hard phones to ensure full compatibility of both the soft phones and hard phones with the project design.

Fedora operating system - which is the plat form in which the asterisk PBX will be run on. Session initiation protocol (SIP) - this protocol was specifically adopted for the design since most products in the market as of today as SIP compliant as against the other protocols especially IAX2.

Asterisk which is an open source - this software transform an ordinary computer into a communication server. **Astra IP Hard phones** (9133i model) - used for the calls between the two servers and also for the configuration of the Voicemail and auto attendant system. X-lite 4 soft phones - to test for its compatibility with the design. IPsec site-to-site VPN; this was also implemented across the VoIP telephony network. Four digit dial plan; this was used in the design of the dial plan numbering system for the asterisk PBX. This was chosen to give room for the company’s expansion or growth; hence accommodating more extensions. Cisco Routers 2800 series, Cisco 2950 switches and PC systems

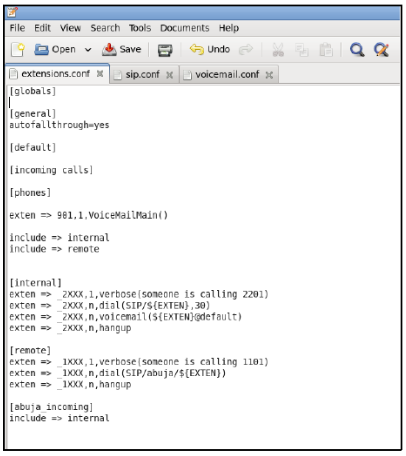
IP addressing scheme -The IP addressing scheme used for the design of the network is a Class C addressing.

Table 2.0: shows the IP addressing scheme for the project design

SN	Description	Abuja Router	Lagos Router
1	Serial Interface IP address S0/0/0	192.168.1.1/24	192.168.1.2/24
2	Fast Ethernet IP address F0/0	192.168.2.1/24	192.168.3.1/24
3	1st extension IP address	192.168.2.2/24	192.168.3.2/24
4	Network IP address	192.168.2.0/24	192.168.3.0/24
5	IP PBX IP address	192.168.2.3/24	192.168.3.3/24
6	1st host system address	192.168.2.4/24	192.168.3.4/24

Asterisk and VoIP phone configurations.

Extension.conf: it contains the dial plan which defines and handles how calls come in, go out and are also routed. The behaviour of the PBX connection can be configured in the file.



```
[globals]

[general]
autofallthrough=yes

[default]

[incoming calls]

[phones]

exten => 981,1,VoiceMailMain()

include => internal
include => remote


[internal]
exten => _2XXX,1,verbose(someone is calling 2201)
exten => _2XXX,n,dial(SIP/${EXTEN},30)
exten => _2XXX,n,voicemail(${EXTEN}@default)
exten => _2XXX,n,hangup

[remote]
exten => _1XXX,1,verbose(someone is calling 1101)
exten => _1XXX,n,dial(SIP/abuja/${EXTEN})
exten => _1XXX,n,hangup

[abuja_incoming]
include => internal
```

Figure 1.0: Extension.conf file

The Extension.conf file is usually located in the etc/asterisk directory as the case may be. Dial plan can be categorized into three main concepts namely

Contexts. The main purpose of the contexts in an Extension.conf file is to keep the different parts of the dial plan from interacting with one another.

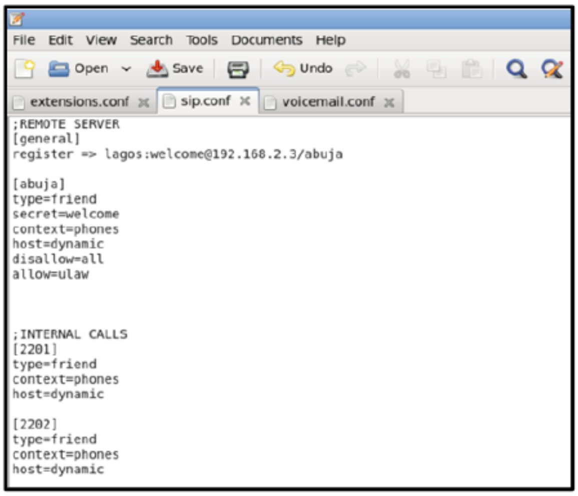
The context also provides some level of security by either permitting or denying a caller’s access to certain features. All the instructions placed after the [general] context are part of the context unless another context is specified. The autofallthrough=yes tells the asterisk to continue running the configurations even when the extension doesn’t have anything to do.

Extensions. An extension comprises of three components: The name, priority and application. These components are separated by commas as shown in an example below; exten => name,priority,application()

Priority. This can be defined as multiple steps in an extension which are normally executed sequentially, for example; *exten => 123,1,answer()* exten => 123,1,hangup(). First priority 1 is to answer the call followed by priority 2 to hang up the call

Application. This is defined as the work horses of the overall asterisk dial plan each performing its specific function, for example answering a call, dialling a number, playing a sound or hanging up a call. Some of the applications include answer(), hangup().

SIP.conf. The authentication of the users and end points including SIP phones is configured in the SIP.conf file. The file is usually used for the determination of calls to be answered or rejected by the user by the asterisk PBX.



```
;REMOTE SERVER
[general]
register => lagos:welcome@192.168.2.3/abuja

[abuja]
type=friend
secret=welcome
context=phones
host=dynamic
disallow=all
allow=ulaw


;INTERNAL CALLS
[2201]
type=friend
context=phones
host=dynamic

[2202]
type=friend
context=phones
host=dynamic
```

Figure 2.0: SIP.conf configuration file

The explanation of the SIP.conf file is detailed below

[abuja]; the content of the context is then name of the SIP device which could also be the extension number

Type = friend; since asterisk PBX is designed for both calls to be placed to the phones and received as well, the type is defined as friend. The other options that can be set under type are;

User; which is mainly for calls leaving the dial plan which is usually through the Dial () application. The type friend is preferred since it defines both the user and the peer.
Host; this option is used to define the users or clients that exist on the network. The asterisk PBX receives a REGISTER packet telling it which IP address the SIP peer is using.

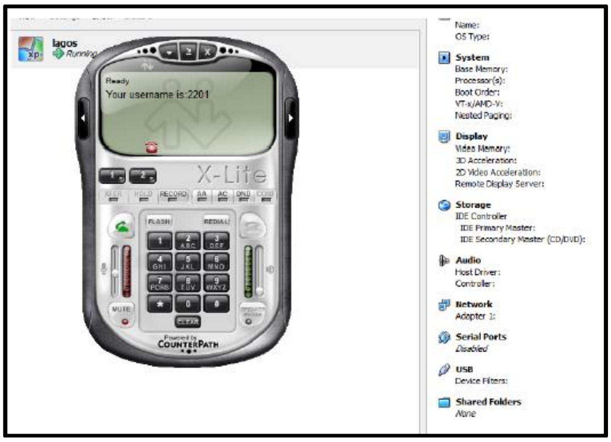
Secret; this sets the password that has to be entered before a client is added to the network. This option also secures an untrusted network by forcing the use of password (secret=password).

Context = phones; this defines the dial context for the user which in this case is phone
Voicemail.conf. This file contains settings used for configuring and customizing Voicemail to meet specific requirements and needs. The Voicemail.conf file is divided into three sections as shown below;
[general] which contains the global configurations of the Voicemail.conf file. [zone messages]; this section deals with corresponding the different time zones together with the local time zones. This is due to the time difference. Context defined

The syntax for defining a mail box is mailbox => password, name,[email,pager_email [options]]] where the mail box number corresponds to the extension number associated with it. Password is that which is assigned to the mail box by the user to have access to the mail box which is updated by the asterisk PBX in Voicemail.conf

Starting and shutting down an asterisk server - Asterisk is usually run on Fedora or Linux operating system as the case may be and depending on choice. The Extension.conf, SIP.conf and Voicemail.conf configuration files are placed into the etc/asterisk folder. The asterisk server is initiated by inputting this command in the command line interface on the fedora server asterisk – vvvvvvvvvvvvvvc which automatically registers the clients and also establish connection.

It can be stopped should the need arise by entering the command stop core gracefully in the command line interface. The registration of the SIP peers is done after successful registration and start up process is completed.

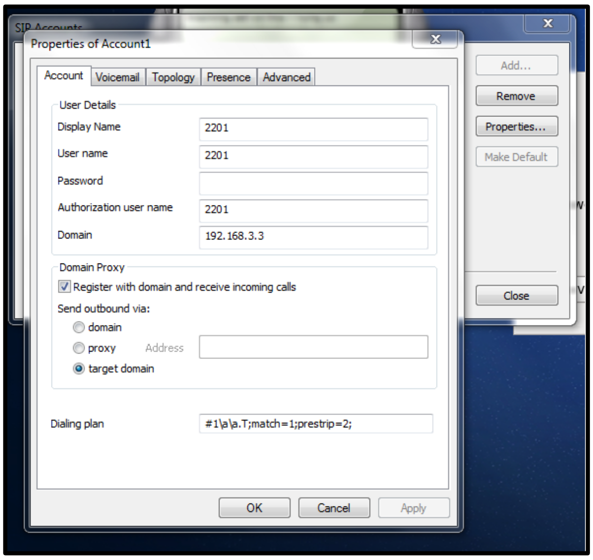


Ready
Your username is:2201

Figure 3.0: registered SIP phone

The Call Process

This is done by entering in the specified parameters such as the IP address of the server, port number, the username and the extension. The configuration of the phone device is shown below in figure.



User Details

Display Name: 2201

User name: 2201

Password:

Authorization user name: 2201

Domain: 192.168.3.3

Domain Proxy

☑ Register with domain and receive incoming calls

Send outbound via:

○ domain

○ proxy Address

● target domain

Dialing plan: #1\a\a.T;match=1;prestrip=2;

Figure 4.0: configured X-Lite 4 soft phone

Security implementation (e.g., IPSec site-to-site security, IPSec VPN).

IPsec site-to-site VPN solution will be implemented across Abuja Lagos branches of the asterisk VoIP based design. The IPsec VPN combines both tunnelling, encapsulation and encryption of the packet transmitted across the network hence ensuring a secured network and also confidentiality of information across the network.
The stages are broken into Initiation of the interesting traffic stage, Internet key Exchange (IKE) phase 1, Internet key Exchange (IKE) phase 2, Transfer of data and Termination of IPSec Tunnel.

Implementation of IPsec VPN in the VoIP telephony network

Initiation of interesting traffic; the interesting traffic here is between the Abuja server and the Lagos server branches respectively. The access list is set up as follows;

Access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0 0.0.0.255
Access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0 0.0.0.255

IKE Phase 1 stage; in this stage the authentication of the IPsec peers by the IKE is carried out. It also carries out security association negotiations and also the creation of a secure channel for the association of the IPsec security. **The commands used for achieving the phase 1 are shown below with explanation of each command line.**

Crypto isakmp enable*; enables the ISAKMP protocol*
Crypto isakmp policy 1*; starts setting up our security associations.*
Encryption 3des*; includes the des encryption*
Authentication pre-share*; includes the authentication type and hashing algorithms*
Group 1*; specifies the group*
Lifetime 86400*; specifies the time before re-authentication starts*
Exit*; exits the mode it's currently in*
Crypto isakmp identity address*; sets how the peer machine is recognized*
Crypto isakmp key washima address 192.168.1.2*; this command sets the key and the peer address*

IKE Phase 2 stage; in this stage, the negotiation of the security association parameters of the IPSec is done and are set in the IPSec security peers. This ensures the protection of the transmitted data between the two servers. The commands used in this stage are shown below;

Crypto ipsec transform-set secured esp-md5-hmac*; encrypts the IPSec tunnel using the des and MD5 hashing algorithm.*
Mode tunnel*; takes us into the tunnel mode*
Crypto map abuja 1 ipsec-isakmp*; IPSec association policy itself*
Set peer 192.168.1.2*; sets the peer IP address*

Set transform-set SECURITY*; used to secure channel*
Set security association lifetime seconds 86400*; time before re-authentication restarts*
Match address 101*; tells the IPSec tunnel about interesting traffic*
Exit*; leave the present mode*
Data transfer*; exchange of data is done between the peers and the keys are saved in the security association file.*
The termination *of the IPsec tunnel is done either by completely deleting or by timing out process.*

6 TESTING

Testing of the VoIP telephony network - The telephony network is tested by ensuring that servers can both dial and receive call among them as shown in the figures below. This can be achieved by using the ping command to test for connectivity between the servers and also dialling the different extension numbers.

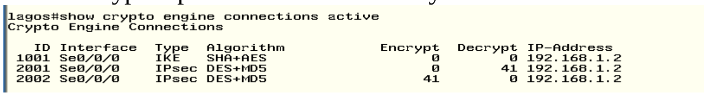
Ping command; this test for connectivity between two points by sending of packets from the source to the destination. 100% delivery signifies success otherwise unsuccessful.
Show IP route command; this command shows the routing table of the router, showing a list of all networks the router can establish connection with.

Testing the IPsec security - The testing of the security solution is to ensure that the IPsec security has been correctly deployed and is fully functional.

The following commands was issued on the router to ensure the network was properly configured with IPsec site to site VPN and is fully functional and operational.

Show crypto IPSec sa; this command is used to show the security association built between the peers on the network. This also shows the tunnel that has been built between the 192.168.1.2 source point and its peer 192.168.1.1. It also shows the encapsulation security payload both at the inbound and outbound.

Show crypto engine connections active; this displays the active security associations on the router along with the number of encrypted and decrypted packets for each security association.

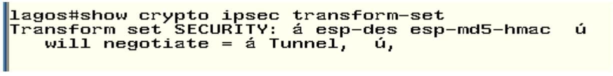


```
lagos#show crypto engine connections active
Crypto Engine Connections

   ID Interface   Type  Algorithm           Encrypt  Decrypt IP-Address
 1001 Se0/0/0     IKE   SHA+AES                   0        0 192.168.1.2
 2001 Se0/0/0     IPsec DES+MD5                   0       41 192.168.1.2
 2002 Se0/0/0     IPsec DES+MD5                  41        0 192.168.1.2
```

Figure 5.0: show crypto engine connections active

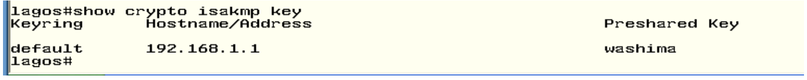
Show crypto IPsec transform-set; this delivers a transform set and shows the transform combination in use.



```
lagos#show crypto ipsec transform-set
Transform set SECURITY: á esp-des esp-md5-hmac  ú
   will negotiate = á Tunnel,  ú,
```

Figure 6.0: show crypto ipsec transform set output

Show crypto isakmp key; this command displays the preshared key. The figure 9 shows the output.

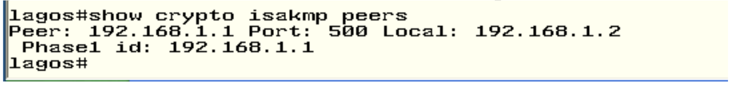


```
lagos#show crypto isakmp key
Keyring       Hostname/Address                          Preshared Key

default       192.168.1.1                               washima
lagos#
```

Figure 7.0: show crypto isakmp key output

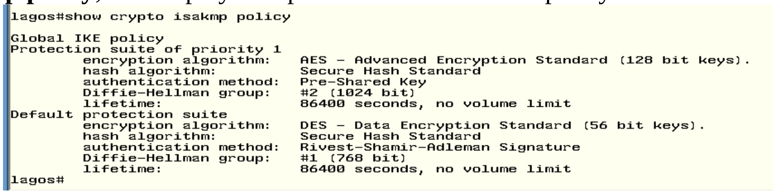
Show crypto isakmp peers; this shows the local IP address and the peer's IP address.



```
lagos#show crypto isakmp peers
Peer: 192.168.1.1 Port: 500 Local: 192.168.1.2
 Phase1 id: 192.168.1.1
lagos#
```

Figure 8.0: show crypto isakmp peers output

Show crypto isakmp policy; this displays the parameter for each IKE policy.

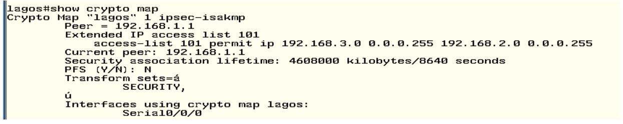


```
lagos#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
lagos#
```

Figure 9.0: show crypto isakmp policy output

Show crypto map; this shows the crypto map configurations.



```
lagos#show crypto map
Crypto Map "lagos" 1 ipsec-isakmp
        Peer = 192.168.1.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
        Current peer: 192.168.1.1
        Security association lifetime: 4608000 kilobytes/8640 seconds
        PFS (Y/N): N
        Transform sets=á
                SECURITY,
        ú
        Interfaces using crypto map lagos:
                Serial0/0/0
```

Figure 10.0: show crypto map output

When the IPsec security was turned off between the branches by using the **no crypto map** command. The Wireshark was able to capture packets. When the IPsec security was turned on the Wireshark could not capture the data since all the information became hidden and fully encrypted by its replacement with the encapsulation security payload (ESP).

7 EVALUATION - Weaknesses, problems and setbacks in the Project Design

Weakness in Asterisk Software: As an open source platform, Asterisk lacks the accountability and guaranteed maintenance, repairs, and upgrades provided by proprietary solutions like Cisco. This risk suggests a preference for proprietary options, though configuration backups can be stored externally.

Effect of Security Solution Deployment: The IPsec VPN uses a shared key for authentication, which compromises security if breached, undermining the tunnelling purpose. Additionally, bandwidth utilization and quality of service issues can degrade overall network performance during calls.

Numbering System Used: The four-digit numbering system may become difficult to manage as departments grow, leading to potential number wastage or shortages.

8 CONCLUSION

The design of the VoIP-based network began with in-depth research and a critical comparison to the existing Public Switch Telephone Network. The advantages of VoIP were discussed with references to various published papers. A comparison of different VoIP protocols led to the recommendation of the SIP protocol for the asterisk VoIP network, supported by research from [21] and [24]. A critical analysis of VoIP attacks, such as man-in-the-middle, call flooding, and spoofing, was conducted. Security methodologies were compared, leading to the recommendation of IPsec site-to-site VPN for strong protection. The design included a dial plan and numbering system based on required extensions. The implementation phase involved configuring VDI images, Oracle VirtualBox, and critical server files (Extension.conf, SIP.conf, and Voicemail.conf). The network was tested through inter-branch calls and IPsec VPN functionality, confirming full security and operational status.

REFERENCES

[1] Clegg, A. (1996) Telecommunications and the internet. International Journal of Telecommunications Policy, Volume 20, Issue 8, pp 545-548.

[2] Arcomano (2002), 'VoIP How to' white paper, Available at http://tldp.org/HOWTO/VoIPHOWTO.html

[3] Abbasi, T., Prasad, S., Seddigh, N., & Lambadaris, I. (2005) A comparative study ofthe SIP and IAX VoIP protocols. In Proceedings of the 2005 Canadian Conference on Electrical and Computer Engineering, pp 179–183, Saskatoon, Canada

[4] Balachandran, A. (2009). A study on VoIP quality and security. International Journal of Computer Networks & Communications, 1(2), 71-84.

[5] Cobley, F., Coward, A. (2004) 'Voice over IP versus Voice of Frame relay', International Journal of Network Management, Volume 4, pp 223-230.

[6] Cisco (2001) Goodbye DES, Welcome AES. The Internet Protocol Journal, Volume 4, Number 2 (Online) Available at: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_42/goodbye_des.html

[7] Cisco (2004) DES/3DES/AES VPN Encryption Module (AIM-VPN/EPII, AIMVPN/HPII, AIM-VPN/BPII Family). (Online) Available at: http://www.cisco.com/en/US/docs/ios/12_2/12_2z/12_2zj/feature/guide/gtaimvpn.html

[8] Smith, J., Brown, K., & Davis, L. (2018). The evolution of communication technology: From legacy phones to VoIP. Journal of Communication Technology, 32(4), 215-230.

[9] Johnson, M., & Wang, H. (2020). Advantages of VoIP over traditional telephony systems. International Journal of Advanced Research in Computer Science and Electronics Engineering, 9(5), 142-156.

[10] Patel, R. (2022). Comprehensive analysis of VoIP features and services. Journal of Telecommunications and Digital Media, 15(2), 87-99.

[11] Patrick Park (2009), 'Voice over IP Security', 1st Edition, Cisco Press, Indiana USA, and ISBN: 978-1-58705-469-3.

[12] Dantu,R., Fahmy, S., Schulzrinne, H., & Cangussu, J.(2009) Issues and challenges in securing VoIP. International Journal of Computer & Security, Volume 28, pp 743-753.

[13] Tucker, G. (2004), 'Voice over IP and Security', SANS Institute Infosec Reading Room, Available at http://www.sans.org/reading_room/whitepapers/voip/voice-internet-protocol-voip-security_1513

[14] Ramachandran (2006), 'VoIP Security: Asserting the Trust boundary, the Global Voice of Information Security, Journal of ISSA, pp 8-13

[15] Dhamankar, R.: Intrusion Prevention: The Future of VoIP Security. White paper. TippingPoint(2005),Available at:http://www.tippingpoint.com/pdf/resources/whitepapers/503160001_TheFuture of VoIP

[16] NIST. "Voice over Internet Protocol (VOIP), Security Technical Implementation Guide." Version 1, Release 1. 13 January 2004. Available at http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V1R1R-4PDF.pdf

[17] Busse, I., Deffner, B., Schulzrine, H. (1996),' Dynamic QoS Control of Multimedia applications based on RTP' International Journal of Computer Communications, Volume 19, pp 49-58.

[18] Chak, H. (2005), 'VoIP principles and Practices', SOMA Network Inc. white paper, Available at: ftp://ftp.rogerwinters.com/usenix05/VoIP_Principles_and_Practice.pdf

[19] Karapantazis, S., Pavlidou, F. (2009), 'VoIP: A Comprehensive Survey on a Promising Technology', International Journal of Computer Networks, Volume 53, pp 2050-2090

[20] Zhang, R., Wang, X., Yang X., & Jiang X. (2010) on the billing vulnerabilities of SIPbased VoIP systems.

[21] Yoon, E., Yoo, K., Kim, C., Hong, Y., Jo, M., & Chen, H. (2010) A secure and efficient SIP authentication scheme for converged VoIP networks. International Journal of Computer Communications, Volume 33, pp 1674–1681.

[22] Geneiatakis, D., Lambrinoudakis, C. & Kambourakis, G. (2007) 'an ontology-based policy for deploying secure SIP-based VoIP services', Journal of Computer & Security, pp.285-297.

[23] Smith, A., & Jones, B. (2017). VoIP Implementations using H.323. Telecommunications Review, 38(4), 221-235)

[24] Alan, B., David, P. (2006), 'Understanding Voice over IP Security', Artech House Inc. ISBN-10: 1-59693-050-0

[25] Brown, D., & Green, R. (2018). Understanding H.323 Network Architecture. Journal of Network and Systems Management, 26(2), 302-319).

[26] Schulzrine, H., & Rosenberg, J. (2002) Internet Telephony: Architecture and protocols– an IETF perspective. Readings in Multimedia Computing and Networking, 2002, pp 635-653.

[27] Katz, D., Tomasz, L., Rich, G., Wayne, W. (2006), 'Want to Know how VoIP networks? Protocols Codecs and More. EE Times-India.

[28] Cao, J., Mark, G. (2008), 'Performance evaluation of VoIP services using difference CODECS over a UMTS Network', IEEE Telecommunication Networks and Application Conference, Volume 35.

[29] Proakis, J. G., & Manolakis, D. G. (2007). Digital Signal Processing: Principles, Algorithms, and Applications. Pearson Prentice Hall.

[30] Putro, H. (2009), 'Performance of various CODECS related to Jitter Buffer Variation in VoIP using SIP',Electrical engineering Journal, Volume 9, pp1.

[31] Zisiadis, D., Kopsidas,S., & Tassiulas, L. (2008) VIPSec defined. International Journal of Computer Networks, Volume 52, pp 2518–2528.

[32] Kuhn, D.,Thomas, J. ,Walsh, Steffen, F.(2005) National Institute of Standards and Technology; NIST Recommendations of NIST concerning VoIP security; Security Considerations for Voice over IP

[33] Cisco (2007) Voice Security Primer: Protecting the Voice Infrastructure, Call-Management System, Applications, and Endpoints, (Online) Available at: http://www.cisco.com/en/US/solutions/collateral/ns339/ns639/ns641/net_implementation_white_paper 0900aecd80460724.pdf

[34] Stallings (2006), 'Cryptography and Network Security, Principles and practices' 4th edition, New Jersey: Prentice Hall

[35] VOIPSA (2005), 'VoIP Security and Privacy Threat Taxonomy' available at http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

[36] Cao, F.& Malik, S. (2006), 'Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors', IEEE Communications Magazine, Cisco Systems Inc, pp 138-145.

[37] Casteel, J. (2005) Sound Choice for VoIP, Available at http://www.infosecwriters.com/text_resources/pdf/VOIP_JCasteel.pdf

[38] Wang Hoa (2004), 'Network Firewall' Computer Network and Security'

[39] Frankel, S., Karen, K., Ryan, L., Angela, O., Ronald, R., (2005), 'Guide to IPSec VPNs' Available at http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

[40] Kwok T.Fung, 2005, Network security technologies. CRC press USA.

[41] Meggelen, T., Madsen, L., & Smith, J. (2007) Asterisk the future of Telephony, 2nd Edition. Beijing ; Farnham : O'Reilly media

[42] Sinha, R. (2003), 'MPLS-VPN Service and Security, SAN's Institute Infosec Reading Room, Available at http://www.sans.org/reading_room/whitepapers/vpns/mpls-vpn-services-security_1124

[43] Chong, H., & Matthews, H. (2004). Comparative analysis of traditional telephone and voice-over-Internet protocol (VoIP) systems. In Proceedings of the 2004 IEEE International Symposium on Electronics and the Environment, pp 106–111, Phoenix, AR, USA.

[44] Nokia (2003), 'Advantages of SIP for VoIP', Available at http://www.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/whitepaper_sip_for_voip.pdf