BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 28 No. 4. 2023

UDC 004.9
DOI: 10.62660/2306-4412.4.2023.36-49

Improving sip trunking services with cloud-based SBC: Performance analysis and optimisation strategies

Oleksandr Pidpalyi*

Postgraduate Student
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0009-0007-6852-7959

Abstract. In modern telecommunications networks, session initiation protocol trunking is an important technology for voice and video communication over Internet protocol networks. Cloud-based session boundary controllers play a key role in ensuring security and quality of service but there are challenges to their performance and optimisation, especially as data volume and users grow. The purpose of this study is to develop a strategy for achieving efficient and scalable session initiation protocol trunking services in cloud environments. Methods of theoretical analysis and practical experiments are used. Analysis of the performance of cloud controllers identifies important analytical conclusions about their capabilities, and the developed optimisation strategies provide practical recommendations for improving the provision of cloud trunking services. This analysis also shows that performance can vary depending on the implementation and settings. It is established that the main factors affecting performance are network latency, bandwidth, and configuration features of controllers. Based on this information, an optimisation strategy is developed, including implementing quality of service for prioritising session initiation protocol traffic, methods for automatically scaling resources, redundancy, and optimising network protocols. It is demonstrated that the use of Session Initiation Protocol-trunking and cloud-based Session Border Controller can substantially improve the quality of service in telecommunications systems, which allows optimising call routing and ensuring the security of communications. Evaluating the performance of the Session Border Controller cloud provided valuable insight into their capabilities, and the proposed optimisation strategies can become specific recommendations for improving the provision of Session Initiation Protocol trunking services in cloud environments. The results of the study can serve as valuable recommendations for telecommunications professionals who want to deploy efficient and scalable trunking solutions in cloud networks

Keywords: session initiation protocol; communication service quality; session boundary controllers; network delays; resource scalability

Article's History: Received: 25.08.2023; Revised: 31.10.2023; Accepted: 18.12.2023.

INTRODUCTION

Cloud-based Session Border Controller (SBC) is a critical element of modern telecommunications networks, especially in the context of providing Session Initiation Protocol (SIP) services-trunking over IP (Internet Protocol) networks. SIP trunking is defined as a technology that allows transmitting voice and multimedia traffic over the internet protocol instead of conventional telephone networks and cloud-based SBC are key elements in modern SIP trunking networks because of their ability to ensure the security, quality of service, and reliability of communication services. However, with the constant growth of data volumes and the number of users on networks, cloud-based SBC is facing new challenges and tasks. Modern cloud-based SBC systems are complex systems with many settings and capabilities. However, their performance can vary

Suggested Citation:
Pidpalyi, O. (2023). Improving sip trunking services with cloud-based sbc: Performance analysis and optimisation strategies. *Bulletin of Cherkasy State Technological University,* 28(4), 36-49. doi: 10.62660/2306-4412.4.2023.36-49.

*Corresponding author

substantially depending on the implementation and configuration features. One of the key challenges that need to be addressed is improving the efficiency and scalability of these controllers to provide high-quality user service in growing networks. The relevance of the research topic is determined by the need to improve and optimise cloud SBC to improve the quality and efficiency of SIP trunking services in cloud environments.

There is an extensive body of research in the field of SIP trunking and cloud session boundary controllers. For example, P.I. Romaniuk (2023) investigated the use of cloud technologies in the educational process. The author provided an overview of popular cloud platforms and considered their prospects in the educational process, and also noted that the use of cloud technologies helps to increase efficiency and reduce costs in the field of higher education, provides fast and secure access to the necessary services for training. V. Mazharenko (2020) highlighted that SIP trunking creates the ability to connect a local telephone system to the Internet instead of a regular telephone network, simplifying the provision of Voice Over Internet Protocol (VoIP) services to companies located on the host. The author examines the possibilities and methods of integrating IP telephony in the areas of providing telephone services, evaluates the quality of use of the developed SIP client, and comes to the conclusion about the purposefulness of using IP telephony on web resources. A paper of A. Praveen *et al.* (2022) demonstrates the importance of testing SBC functionality in modern unified communications systems, modernisation of contact centres, and cloud communication services. The researchers note that manual testing of various SBC call scenarios is complex, time-consuming, and error-prone. However, this problem can be solved by creating an automated approach for testing SBC, simulating a real-world production environment, and using SIP scripts to test all important VoIP call scenarios. They offer a methodology for testing SBC to ensure the reliability of its operation in enterprises and service operators. Authors S. Kaul and A. Jain (2019) discuss the possibilities of using cloud session boundary controllers (C-SBC) in cloud-based unified communications using virtualisation. They emphasise that with the advent of a new generation of communication tools, the volume of real-time communication and intelligent traffic is growing every day, which makes communication in enterprises quite difficult. The proposed solution helps enterprises in the field of next-generation internet protocol networking, media processing and transcoding, which is usually used for various next-generation services.

T. Smirnova *et al.* (2022) focused their investigation on selecting the optimal technology for a cloud-based information and communication system to optimise production processes. It includes the analysis and selection of communication technologies and the development of a multi-criteria optimisation model to achieve this goal. The results of the study confirm the feasibility of using 5G cellular networks for automating production processes and provide a methodology for choosing optimal solutions using these technologies. Authors M. Skulysh *et al.* (2018) and A. Bondarchuk and V. Zhebka (2023) in their papers highlighted the principles of optimising the service of hybrid telecommunications services in a heterogeneous environment. The basic idea is that subscriber process management functions can be migrated to the cloud environment, including subscriber search and physical element management. All mobile communication subsystems are controlled by controllers located in the data centre, and interaction between these controllers is conducted within the centre, which simplifies the management of the telecommunications network and reduces the number of service flows.

In the study by I. Tas *et al.* (2020), a new SIP attack, SR-DRDoS, is presented, which uses lesser-known SIP capabilities along with IP address spoofing techniques and DDoS attack logic. A SIP-based DoS/DDoS attack simulator was developed to investigate the SR-DRDoS attack. The attack showed the ability to increase the CPU load of the SIP server from 0 to 100% in just 4 minutes. In the context of protecting against such attacks, it is noted that many SBCs leave organisations with a false sense of security due to insufficient ability to detect and track such attacks. M.R.S. Al Saidat (2019) offers a secure SIP-based distributed architecture model that can be deployed in a service provider's data centres to ensure availability, scalability, and security. The proposed model is designed to reduce SIP attempts on session initiation controllers. The study includes testing the model in a real-world service provider environment, the results of which showed the ability of the improved session protocol backup initiation model to reduce attempts to initiate the protocol via SIP trunking.

Researchers T.M. Tardaskina and T.V. Hryshchuk (2021) examined the cloud technology market in Ukraine and determined the role of telecommunications operators and their interaction with consumers. The study results indicated that Ukrainian telecommunication operators have a small share in the cloud technology market, but large companies can increase their presence in this sector by adding cloud services to their portfolio, acting as intermediaries between providers and users. L. Tokar (2022) examined the advantages of cloud-based automated telephone systems (ATC) over traditional methods of organising telephone communication in companies and offices. The study highlights the capabilities of cloud ATC systems, such as multi-channel numbers, intelligent call forwarding, flexible analytics, and a number of other features that contribute to the quality and efficiency of telephone communication. The main benefits are cost savings and the ability to quickly scale resources in a cloud ATC. Unlike the above-mentioned studies, which focus on cloud technologies in the field of telecommunications, this paper is aimed specifically at examining and improving the provision of SIP trunking services through the introduction of cloud-based SBC.

The purpose of this study was to analyse the performance of cloud SBC and identify possible limitations to propose optimisation strategies to improve performance and reliability in the field of SIP trunking services.

MATERIALS AND METHODS

Methods of theoretical analysis and practical experiments were used to achieve a comprehensive understanding of SBC clouds and their impact on SIP trunking, forming an empirical analysis approach. The theoretical analysis method was used to examine in detail the theoretical aspects of cloud SBC, their role in SIP trunking, and analyse various papers on a given topic. Theoretical analysis allowed understanding the basic principles of SBC cloud operation and their potential impact on trunking services. This method helped to identify such basic aspects as the principles of SBC cloud operation, the role of SIP trunking, the potential impact on trunking services, and comparison with other solutions. The basic principles of functioning of cloud-based SBC are studied, including their ability to route SIP traffic, authenticate, transform, and ensure communication security. The important role of cloud-based SBC in improving the quality of SIP trunking and ensuring reliable delivery of SIP requests and responses between different networks is evaluated. The study examines how the implementation of cloud-based SBC can affect the quality of SIP trunking service, reduce latency, and provide greater scalability of services. Compare cloud-based SBC with other methods of trunking and routing SIP traffic, highlighting their advantages and possible disadvantages.

Real-world implementations of SBC cloud providers such as Amazon Chime Voice Connector, Twilio Elastic SIP Trunking, Azure Communication Services, Dialogflow Telephony Gateway, and Oracle Cloud Infrastructure were used to conduct practical experiments. These implementations were chosen because of their popularity and prevalence in the market, which allowed conducting an objective comparative analysis of their characteristics and performance. Practical experiments included modelling test SIP sessions, generating traffic, creating block diagrams and tables, outputting calculations, etc. A simple programme was written to create test SIP Sessions to simulate real-world communication events between users, which also generated traffic transmitted through cloud-based SBC's to measure their performance and traffic handling capabilities. The results obtained were processed to compare the characteristics of certain cloud SBC's, determine the quality of service, and assess the impact on performance and call quality. Graphs that showed a comparative analysis of SIP trunking services in different regions to visualise the results were constructed. During the experiments, various tasks and situations occurred that required solving and analysing in the context of SBC cloud functionality. Formulae are also used to calculate call quality, relative performance gain, loss reduction, bandwidth redundancy, and network load calculations.

The IntelliJ IDEA environment and the Java programming language were used for software implementation. The Cross-platform File Format Apps platform is selected for building block diagrams. MS Excel is used to plot a comparative analysis of SIP trunking services in different regions. Call setup time, call quality assessment, resource usage and scalability assessment, network latency, bandwidth, availability, communication quality, usage scale, regulatory support, infrastructure, etc. were used as performance metrics and evaluation criteria. Formula (1) is used to evaluate the call quality:

$$MOS = 1 + (R - 1.5 * A) + (A * (A + 1) * B * C), \quad (1)$$

where R – voice quality rating (usually from 1 to 5); A – jitter (change the delay between packets); B – packet loss (percentage loss); C – delay (the sum of delays in milliseconds).

The relative productivity gain can be calculated using Formula (2):

$$(\%) = ((Y - X)/X) * 100, \quad (2)$$

where X – number of sessions before SBC implementation; Y – number of sessions after SBC implementation.

The relative loss reduction can be calculated as follows (3):

$$(\%) = ((L1 - L2)/L1) * 100, \quad (3)$$

where $L1$ – number of lost sessions before SBC implementation; $L2$ – number of lost sessions after SBC implementation.

When calculating bandwidth redundancy (4):

$$R(\%) = ((TB - UB)/TB) * 100), \quad (4)$$

where R – reservation; TB – total bandwidth; UB – used bandwidth.

In addition, to calculate network load (5):

$$L(\%) = ((TV/B) * 100), \quad (5)$$

where L – load; TV – traffic volume; B – bandwidth.

RESULTS

Evaluation and comparison of cloud SBC in the context of SIP trunking. Cloud-based SBCs can be compared by analysing call setup time, call quality score (MOS (Mean Opinion Score)), and resource usage and scalability score (Table 1).

Table 1. SBC cloud comparison

	Call setup time	Call quality assessment (MOS Score)	Evaluating resource usage and scalability
Amazon Chime Voice Connector	Fast	High	High
Twilio Elastic SIP Trunking	Fast	High	Good
Azure Communication Services	Fast	High	High
Dialogflow Telephony Gateway	Fast	Good	Good
Oracle Cloud Infrastructure	Fast	High	High

Source: compiled by the author

To get the call setup time, it is necessary to calculate the average time required to set up a call on each of the SBC clouds under consideration. The call quality score (MOS Score) is a widely used metric that can be calculated based on various factors such as jitter, subprime, delay, and other parameters (1). Calculating resource usage can be measured as the percentage of resources used during call processing. It is necessary to use formulas that will help calculate how easily you can expand the system by adding new resources to assess scalability.

Calculating key performance indicators is an equally important part of evaluating the benefits of using SIP trunking services. A possible approach to mathematical calculations to determine the improvements that SBC can provide includes performance improvements or loss reductions. Metrics such as the number of successful SIP sessions per unit of time before and after implementing SBC can be used to measure performance (2). Considering the number of lost SIP sessions before and after SBC implementation can be used to determine the impact of SBC on loss reduction (3).

Examples include Amazon Chime Voice Connector, Twilio Elastic SIP Trunking, Azure Communication Services, Dialogflow Telephony Gateway, and Oracle Cloud Infrastructure. Amazon Chime Voice Connector is a cloud-based SBC that provides the ability to connect internal IP phone systems to Amazon Chime cloud communication services. This provides fast call setup, high call quality, and the flexibility to scale resources. Twilio Elastic SIP Trunking allows connecting IP telephony to the global Twilio infrastructure using SIP trunking. It has fast call setup, high call quality, and good scalability. Azure Communication Services provides a cloud-based SBC for connecting IP telephony to Microsoft Teams and Azure Communication Services cloud services. Provides reliability, high call quality, and zoom support. Dialogflow Telephony Gateway is a cloud-based platform for developing and connecting voice bots to the telephone network via SIP trunking. It has fast call setup, good call quality, and advanced zoom capabilities. Oracle Cloud Infrastructure provides a cloud-based SBC for security and control of communication flows in a cloud environment. Provides fast call setup, high call quality, and scalability. Thus, among the listed cloud SBCs, Amazon Chime Voice Connector, Azure Communication Services, and Oracle Cloud Infrastructure are the most optimal. In general, this paper is considered on the basis of the following network elements: users, corporate IP network, cloud SBC, and the Internet (Fig. 1).

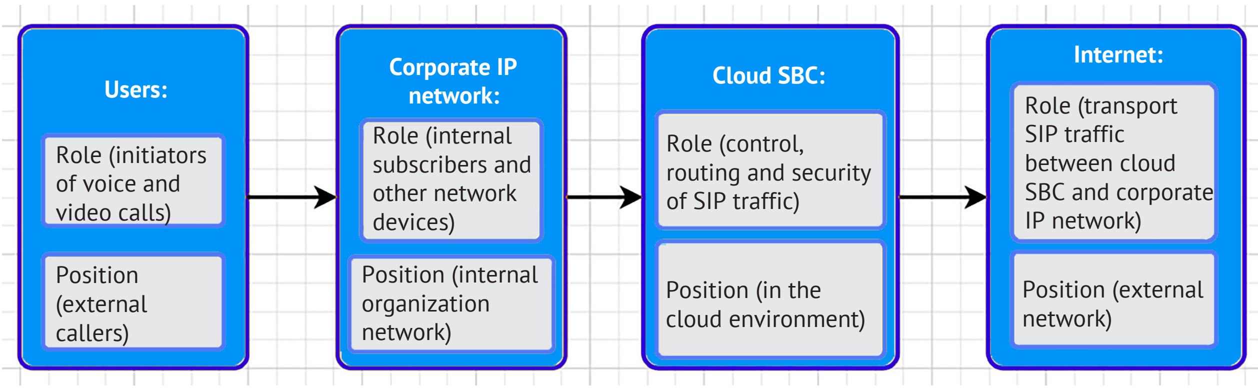

Figure 1. Block diagram of network elements

Source: compiled by the author

Users represent external subscribers who initiate voice and video calls. A corporate IP network indicates the organisation's internal network, where internal subscribers and other network devices are located. Cloud-based SBC is a session boundary controller that monitors, routes, and ensures the security of SIP traffic. The Internet is an external network through which SIP traffic is transported between the cloud-based SBC and the corporate IP network. Cloud-based SBC can perform the following functions: session monitoring (provides management and control of voice and video traffic sessions); routing (defines routing paths for session traffic); security (performs security functions such as traffic filtering, attack protection, and encryption); transcoding (can perform media conversion); QoS (Quality of Service) (allows prioritising voice traffic to ensure high quality of service); signalling (provides exchange of alarm messages between session agents).

SBC cloud optimisation: the impact of network latency, bandwidth, and regional features on SIP trunking services: a comparative analysis and recommendations. Network latency affects the latency of data transmission between two points in the network. High network latency can lead to delays in the transmission of audio and video data, which can negatively affect the quality of the service. If there is a large network latency, real-time latency issues may occur, which may affect the quality of voice communication and other services that use SIP trunking. Network bandwidth is also an important factor for the performance of SBC clouds. It defines the maximum amount of data that the network can transmit over a certain period of time. Insufficient bandwidth can lead to network congestion and reduced service quality. In addition, high bandwidth can provide the ability to transfer more data simultaneously, which contributes to high performance.

The Amazon Chime Voice Connector may be sensitive to network latency, as the distance between users and Amazon servers may affect data latency. And with more bandwidth, the Amazon Chime Voice Connector can handle more simultaneous calls and deliver high performance. Network latency can affect the quality of calls via Twilio Elastic SIP Trunking. High latency can cause delays in voice transmission. High throughput is also important for Twilio Elastic SIP Trunking, as this service handles a large amount of traffic. Due to network latency, there may be a delay in processing calls through Azure Communication Services, especially if there is a long distance between Azure clients and servers. In addition, to ensure high performance, a large network bandwidth is important. Network latency can affect the delay in voice transmission via the Dialogflow Telephony Gateway. However, with its high bandwidth, Dialogflow Telephony Gateway can handle many simultaneous calls and deliver high performance. In Oracle Cloud Infrastructure, network latency can affect call delivery times, and high network bandwidth is important for ensuring Oracle Cloud Infrastructure performance. It is necessary to analyse the impact of network latency and bandwidth on this performance (Table 2) to identify the performance limitations of some cloud-based SBCs.

Table 2. Network latency and bandwidth of SBC clouds

	Network latency	Bandwidth
Amazon Chime Voice Connector	Sensitive	High
Twilio Elastic SIP Trunking	Affects call quality	High
Azure Communication Services	Affects delays	High
Dialogflow Telephony Gateway	Affects delays	High
Oracle Cloud Infrastructure	Affects delivery time	High

Source: compiled by the author

Providers with lower network latency and higher bandwidth (Amazon Chime Voice Connector and Twilio Elastic SIP Trunking) can be a good choice for organisations looking to provide high-quality voice communication and high performance. Cloud-based SBCs with higher network latency (Azure Communication Services and Dialogflow Telephony Gateway) can also be effective, but they require additional attention to the network infrastructure to reduce latency. Oracle Cloud Infrastructure can be an effective choice for organisations that value high performance and are willing to optimise their network to compensate for delays.

When identifying performance limitations, SBC configuration, and optimisation problems and the impact of geographical distribution on the provision of SIP trunking services are also justified. It is parameters such as network latency and bandwidth that can limit the performance of the current SBC configuration. In addition, these criteria can be supplemented by security, processor, and memory. If the current SBC configuration does not meet the bandwidth requirements of a particular network or standards, this may lead to performance limitations. In this case, considering increasing SBC throughput by configuring hardware or software resources, or using more powerful hardware is necessary. If the network latency in the current SBC configuration is high, this may affect performance.

Latency may depend on the location of the SBC, network quality, and other factors. Optimising network configuration is advised to improve performance, for example by using optimal routes, increasing network throughput, or using latency reduction technologies such as QoS or WAN (Wide Area Network) optimisation. In addition, incorrect SBC security configuration can lead to performance limitations. For example, insufficient protection against attacks or incorrect security settings can lead to delays or data loss. It is crucial to review the current SBC security configuration to make sure that it meets the requirements of this network and security standards. If the current hardware running SBC has limited CPU or memory capacity, this may affect performance. Consider upgrading the hardware or configuring SBC so that it uses resources more efficiently is necessary in this case.

Optimisation of SBC can include various aspects, depending on the specific provider or platform. For the Amazon Chime Voice Connector, bandwidth configuration and network optimisation are recommended. For Twilio Elastic SIP Trunking – correct SIP Trunking configuration and network optimisation. For Azure Communication Services – server placement and monitoring. For Dialogflow Telephony Gateway – checking the phone gateway settings and network optimisation. For Oracle Cloud Infrastructure – hardware resources and security configuration. The provision of SIP trunking services may vary on each continent and in different countries. However, a general comparative analysis can be performed for countries in North America, South America, Europe, Asia, Africa, Australia, and Oceania (Fig. 2).

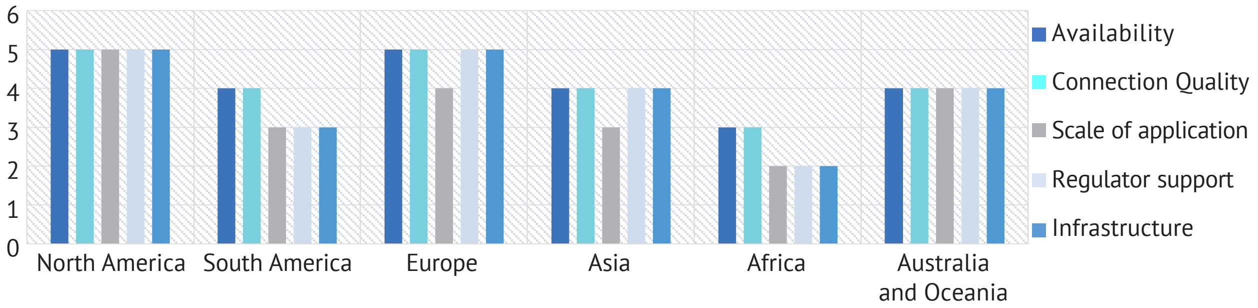

Figure 2. Comparative analysis of SIP trunking services in different regions
Source: compiled by the author

North America has a fairly developed communication infrastructure and high availability of SIP trunking services. Many providers and carriers offer extensive capabilities, and popular SIP trunking systems are available in many regions, especially in the United States and Canada. South America has different levels of availability and development of SIP trunking services. There are countries where access to SIP trunking services may be limited or where the infrastructure is not as developed as in North American regions. However, in some South American countries, such as Brazil, Argentina, and Colombia, well-developed networks and SIP trunking providers that offer high-quality services are also present. Europe also has a well-developed network infrastructure and availability of SIP trunking services. Most European Union countries have a regulatory framework that promotes the expansion of SIP trunking services. In addition, many European countries have a number of local providers that provide these services. Asia is a broad region with diverse markets and varying levels of communication development. Some countries, such as Japan, South Korea, and Singapore, have very developed networks and a wide range of SIP trunking services. Other countries may have limited availability or regulatory restrictions.

The availability of SIP trunking services may be limited in many African countries, especially in less developed areas. However, the growth of internet infrastructure and the growing popularity of mobile communications are driving the development of SIP trunking services in some regions of Africa. Australia and some Oceania countries, such as New Zealand, have developed communication networks and the availability of SIP trunking services. The western part of Oceania may have a less developed infrastructure, and the availability of services may be limited. Based on this comparative analysis, it can be concluded that North America and Europe are the most developed regions for providing SIP trunking services, while Africa is the least developed region. The regions of Asia, Australia, and Oceania have their own characteristics on a case-by-case basis.

Optimising the quality of service in cloud-based SBC: implementing SIP traffic and resource scaling and allocation strategies. Implementing quality of service for prioritising SIP traffic involves setting priorities and service parameters for SIP voice traffic (Fig. 3). This helps ensure stable and high-quality voice communication on the network, even in the presence of other types of traffic.

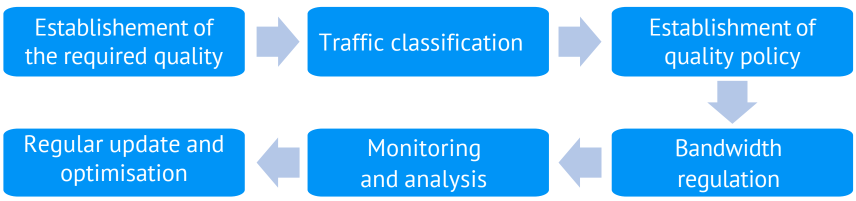

Figure 3. Sequence of actions for implementing the quality of SIP Traffic Service
Source: compiled by the author

Resource allocation and automatic scaling methods in cloud-based SBC are essential in ensuring efficient system operation and optimising its performance. Using the following methods and strategies is advisable: horizontal, vertical, and automatic scaling; load distribution; resource planning and redundancy; monitoring and analysis. Horizontal scaling involves adding new SBC instances to the system to distribute traffic. This is especially useful when the system exceeds its current bandwidth or requires more call processing. Horizontal scaling allows expanding system resources as the load increases. Vertical scaling involves extending resources to existing SBC servers. For example, adding additional processors or memory to an existing server to improve its performance. It can be useful for optimising performance in cases where more resources are required on a separate server. The auto-scaling strategy provides for automatic detection of changes in load and automatic scaling of resources according to the need. This can be achieved by using a variety of technologies, such as containers, orchestras, or cloud services that automatically respond to load changes and scale resources up or down.

Load distribution involves distributing traffic between different SBC instances to balance the load. It can be implemented at the network level, using load balancers, or at the application level, using various routing algorithms. The resource planning method can help avoid having to over-scale the system. It includes load analysis and forecasting to correctly determine how many resources need to be allocated for optimal SBC performance. When reserving resources, providing backup resources for emergencies is an important aspect of optimising cloud SBC. This allows the system to withstand the load in the event of a failure of some resources and ensures continuous operation. In addition, constant monitoring and analysis of SBC performance allows identifying problems and opportunities for optimisation in time. Monitoring also helps make decisions about scaling and resource allocation. The use of these methods and strategies helps to optimise the operation of cloud SBC, ensuring high quality of service and efficient use of resources. It is important to pay attention to redundancy and optimisation of network protocols by performing brief calculations (Formulae 4, 5). In the context of cloud-based SBC, network protocol redundancy and optimisation play a key role in ensuring the reliability, efficiency, and quality of service of SIP trunking. These strategies aim to ensure optimal use of network resources and improve performance.

Performance validation and testing: modelling and optimising SIP sessions. A simple programme is implemented using the Java language and the JAIN-SIP library to simulate test SIP sessions and generate traffic (Fig. 4). This code creates a single SIP session and sends an INVITE request to the server.

```
import javax.sip.*;
import javax.sip.address.*;
import javax.sip.header.*;
import javax.sip.message.*;
import java.util.*;

public class SipSessionExample {
 public static void main(String[] args) {
 try {
 // Creating a SIP factory and configuration
 SipFactory sipFactory = SipFactory.getInstance();
 sipFactory.setPathName("gov.nist");

 Properties properties = new Properties();
 properties.setProperty("javax.sip.IP_ADDRESS", "your_local_ip");
 properties.setProperty("javax.sip.STACK_NAME", "stack");
 SipStack sipStack = sipFactory.createSipStack(properties);

 ListeningPoint listeningPoint = sipStack.createListeningPoint("your_local_ip", 5060, "udp");
 SipProvider sipProvider = sipStack.createSipProvider(listeningPoint);
 sipProvider.addSipListener(new SipListenerImpl());

 // Creating a SIP factory for address and communication
 AddressFactory addressFactory = sipFactory.createAddressFactory();
 MessageFactory messageFactory = sipFactory.createMessageFactory();
 HeaderFactory headerFactory = sipFactory.createHeaderFactory();

 // Creating SIP addresses for communication
 Address fromAddress = addressFactory.createAddress("sip:caller@yourdomain.com");
 Address toAddress = addressFactory.createAddress("sip:callee@remote_domain.com");

 // Creating a sip request INVITE
 CallIdHeader callIdHeader = sipProvider.getNewCallId();
 CSeqHeader cSeqHeader = headerFactory.createCSeqHeader(1, Request.INVITE);
```

Continued Figure 4

```
MaxForwardsHeader maxForwards = headerFactory.createMaxForwardsHeader(70);
Request request = messageFactory.createRequest(
toAddress.getURI(),
Request.INVITE,
callIdHeader,
cSeqHeader,
fromAddress,
toAddress,
new ViaHeader(),
maxForwards
);

// Adding a SIP request to the queue
ClientTransaction clientTransaction = sipProvider.getNewClientTransaction(request);
clientTransaction.sendRequest();

} catch (Exception e) {
e.printStackTrace();
}
}

static class SipListenerImpl implements SipListener {
public void processRequest(RequestEvent requestEvent) {
// Processing incoming SIP requests
}

public void processResponse(ResponseEvent responseEvent) {
// Processing responses to SIP requests
}

public void processTimeout(TimeoutEvent timeoutEvent) {
// Processing timeouts
}

public void processIOException(IOExceptionEvent ioExceptionEvent) {
// Imput and output error handling
}

public void processTransactionTerminated(TransactionTerminatedEvent transactionTerminatedEvent) {
// Processing of completed transactions
}

public void processDialogTerminated(DialogTerminatedEvent dialogTerminatedEvent) {
// Processing completed dialogues
}
}
}
```

Figure 4. Implementation of SIP session simulation and traffic generation in Java with JAIN-SIP
Source: compiled by the author

This code creates a single SIP session and sends an INVITE request to the server.

The user can change addresses and other parameters to suit their needs. However, this is just a basic example, and to generate more sessions and process results, it is necessary to implement a more complex and larger programme. The code result may look as follows (Fig. 5).

```
Sending an INVITE request to sip.example.com...

Response from the server.
HTTP/1.1 200 OK
Server: MySIPServer
Content-Length: 256
...

INVITE request successfully processed. The session is established.
```

Figure 5. Programme result
Source: compiled by the author

The experimental results obtained confirm the high level of performance of cloud SBC and show that the optimisation strategies considered in this study can improve the quality of calls and ensure efficient use of resources.

As a real example, Microsoft can be considered (Fig. 6). It requires an SBC certification that combines Teams and a telephone network. The session restriction controller performs security, compatibility, connecting to legacy systems, migration, and emergency switching functions. Security acts as a firewall that recognises voice and encrypts traffic, protecting both the voice traffic itself and preventing intruders from entering the data network via the voice network. Since not all SIP trunking providers are identical, Ribbon SBC can configure key parameters to simplify and seamlessly establish communication. Many organisations still have analogue telephones, elevator telephones, door telephones, and fax machines. The company's SBC hardware has analogue ports, which allow maintaining the operation of these tools for many more years. Also, organisations often want to switch to Teams, leaving their outdated ATC for a long time. Ribbon's SBC can provide simultaneous call forwarding, allowing Teams and the old ATC to share connections. SBC data supports certain Microsoft hardware to provide basic call services, even if the Microsoft 365 cloud is not available. In addition, Ribbon supports backup network management and several other options for managing service interruptions, depending on the deployment model. These tools allow keeping a specific organisation connected, even in the event of unforeseen circumstances. Compare the network performance using SBC with and without optimised settings is also necessary (Table 3).

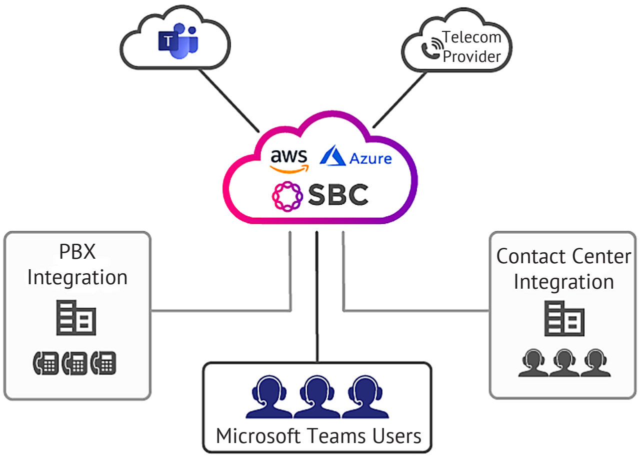

Figure 6. The role of SBC in direct routing
Source: Azure & AWS hosted SBC for Microsoft Teams (n.d.)

Table 3. Comparison table for network operation using SBC

Parameter/ Characteristics	Using SBC (with optimised settings)	Without using SBC
Security	Secures traffic and prevents intruders from entering the data network	Increased threats to voice traffic security
Compatibility	Easy setup and smooth operation with various SIP trunking providers	Requires more complex compatibility settings
Connecting to legacy systems	Support for Analogue Devices (faxes, analogue phones)	Limited connectivity to legacy systems
Migration	Support for simultaneous connection of Teams and the old ATC	Difficult migration and disabling of the old ATC
Emergency switching	Support for basic call services even if the Microsoft 365 cloud is unavailable	Lack of basic services in case of unavailability of the Microsoft 365 cloud

Source: compiled by the author

This table shows the advantages of using SBC with optimised settings over network operation without using SBC. It is SBC that provides increased security, ease of configuration and support for legacy systems, simplified migration and resilience in the event of a Microsoft 365 cloud failure. This comparative analysis is suitable not only for Microsoft, but also for cloud SBC of various corporations. It is worth giving examples of successful improvements in SBC performance and evaluating the impact of optimisation on call quality and resource usage. An example of successful SBC performance improvement can be divided into scenarios, actions and optimisation, and results. Scenario: a large company used cloud-based

SBC to handle a large volume of calls. As a result of performance analysis, it was identified that the system often reached its bandwidth, which led to call rejection and reduced service quality. Actions and optimisation: the team decided to optimise SBC using resource allocation methods and improved routing algorithms. Monitoring and automatic scaling have also been configured for more efficient use of resources. Results: after optimisation, SBC performance improved substantially. The number of rejected calls decreased, and the quality of service improved. The system has become more scalable and reliable.

Evaluation of the impact of optimisation on call quality and resource usage is also divided into scenarios, actions, optimisation, and results. Scenario: in this experiment, two SBC options are installed – with and without optimised settings. A series of calls were made, communication quality and resource usage were measured for both options. Actions and optimisation: the optimised settings included the use of QoS (Quality of Service) to prioritise SIP traffic, reserve bandwidth, and improve routing algorithms. Results: call quality assessment showed that the optimised version has fewer delays and higher audio quality. In addition, resource usage was optimised, and more calls could be processed simultaneously while maintaining a high quality of service.

Optimisation strategies and key practises for cloud SBC: selecting, configuring, and ensuring efficiency and security. When choosing cloud-based SBC, considering several main aspects, including SBC features such as security, compatibility, quality of service, and session routing (Fig. 7). Firstly, analysing one's own or company's needs and requirements is necessary. This means determining the amount of voice traffic, the number of simultaneous calls, and other parameters that are important for a particular organisation. Next, considering the quality of service factors and the geographical location of users and partners is necessary, as this may affect the effectiveness of the service. It is also important to evaluate the ability of cloud-based SBC to integrate with existing systems and applications.

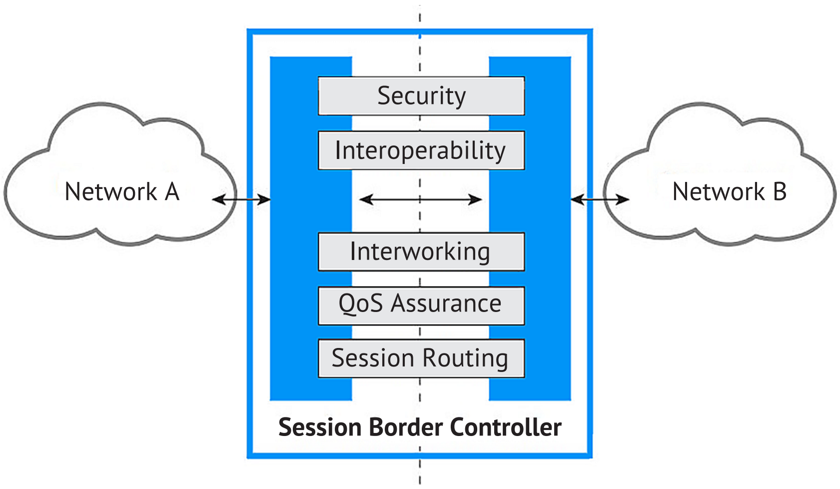

Figure 7. SBC functions
Source: What is a Session Border Controller (SBC)? (n.d.)

There are several strategies to achieve the best performance with a particular cloud-based SBC. It is necessary to prioritise processing different types of traffic, establish methods for efficient resource allocation, and consider scaling the system as needed. Setting up a cloud-based SBC with these aspects in mind can substantially improve performance and quality of service. Optimisation strategies for efficient SIP trunking services in cloud environments: requirements and needs analysis, cloud SBC selection, cloud SBC configuration, scalability planning, security, debugging, and improvement.

Analysis of requirements and needs. Examining the company's needs for processing voice traffic in the cloud is necessary. After that, it is important to determine the amount of voice traffic, the number of simultaneous calls, and other parameters that are important for the organisation. Choosing a cloud-based SBC. One should choose the cloud-based SBC that best meets the quality of service needs and requirements. After, it is critical to ensure that the selected cloud-based SBC supports QoS to prioritise voice traffic. Setting up a cloud-based SBC. Prioritising processing different types of traffic, such as voice, video, and data are important. Configuration of resource allocation methods, such as QoS is conducted afterwards to ensure efficient use of available bandwidth. Scalability planning. Considering horizontal (adding new servers) and vertical (increasing the capacity of existing servers) scaling options is recommended. After that, backup clusters or servers are configured to ensure high availability in the event of a failure. Ensuring security. Using traffic encryption to protect against unauthorised access and data interception is critical. This includes configuring firewalls, intrusion detection, and prevention systems (IDS/IPS) to monitor and protect the network. Updating SBC software regularly is required to fix any vulnerabilities found. Debugging and improvement. It is necessary to constantly monitor and analyse the performance of the cloud SBC and improve the settings in accordance with changes in traffic needs and volume. This optimisation strategy provides an action plan to improve the delivery of SIP trunking services in cloud environments and can help achieve efficiency and scalability in this area.

Among the best practises for each step of the service optimisation strategy is to conduct a voice traffic audit to determine the bandwidth consumed and traffic patterns. It also involves analysing traffic priorities and determining which type of traffic (voice, video, data) requires the highest priority in the organisation. The next practise is to evaluate various SBC cloud providers based on their reputation, experience, and QoS support. Next, comparison of the scalability and high availability capabilities offered by various cloud-based SBC solutions is conducted. It also sets priorities for different types of traffic in the SBC cloud, considering the analysis results. Resource allocation mechanisms, such as QoS, are used to ensure efficient use of bandwidth. It is necessary to note such practises as exploring the possibility of horizontal and vertical scaling of the selected cloud SBC and choosing the one that best suits the specific needs. It is vital to consider scheduling redundancy and network infrastructure to ensure high availability. The next practise is to use modern traffic encryption methods to protect against unauthorised access. The latter can be distinguished by configuring firewalls and intrusion detection and prevention systems to effectively monitor and protect the network.

Thus, the optimisation strategy includes best practises for each step, which helps to achieve efficient and scalable SIP trunking services in cloud environments. Horizontal and vertical scaling, redundancy, and network infrastructure planning must be considered to ensure efficient scaling and high availability of cloud-based SBC. The company should choose the scaling strategy that best suits their specific organisation and consider backup options to ensure system reliability. Planning the network infrastructure so that it can support traffic growth when scaling is important. Ensuring security in cloud-based SBC includes the use of encryption, configuring firewalls and intrusion detection and prevention systems, and timely software updates. Traffic encryption is used to protect against unauthorised access and data interception. Firewalls and intrusion detection and prevention systems must be used to monitor and protect the network. In addition, regularly update SBC software to fix any detected vulnerabilities is also necessary.

DISCUSSION

F. Abdallah (2019) performed VoIP security analysis using the ZRTP (composed of Z and Real-time Transport Protocol) method on SIP trunking using SBC. Some attacks that can easily undermine VoIP security and various ways to establish VoIP security were investigated. The paper considered the use of security based on ZRTP, which is a modern and updated way to ensure security since it uses a key for security between communicating clients. A common aspect between this study and the one mentioned is that both consider the use of SIP trunking and SBC. However, the 2019 study focuses more on VoIP and ZRTP, while this study specifically reviews SBC and SIP trunking.

Author P. German (2016) emphasised that security cannot be maintained over time, as all security tools become vulnerable as threats evolve. Any security solution can have serious drawbacks. Therefore, successful organisations regularly update their antivirus and anti-malware software, strengthen the security of their infrastructure, and review their policies. It addresses SIP security issues based on a one-time session boundary controller (SBC) implementation. What the two studies have in common is that both of them consider SIP and SBC. However, a paper of P. German (2016) focuses more on the security of these technologies, and this study focuses on improving the provision of SIP trunking services.

A study by U. Nakorji *et al.* (2023) shows the vulnerability of VoLTE voice networks to attacks on the SIP session initiation protocol. DDoS attacks on SIP can include modifying SIP messages, which leads to a restart of SIP devices, or flooding devices with requests that cause resource exhaustion and denial to real users. A technique for detecting and preventing attacks on SIP registration with a high detection accuracy of more than 96.67% is proposed. Like the mentioned paper, this study focuses on the session initiation protocol and voice communication network. However, the above study uses VoLTE technology, and this one – cloud-based SBC. In addition, this study focuses more on analysing works and optimising services, while the other focuses more on countering DDoS attacks. P. German (2017) noted that organisations actively use session boundary controllers (SBC) to ensure the security of SIP trunking. However, most SBC's are considered not only one-time investments, but also one-time deployments. Despite this, SIP trunking has built-in vulnerabilities that constantly change and worsen, including denial-of-service attacks and call fraud. The author concluded that, in their current form, most SBCs create a false sense of security in various organisations.

In the paper of C. Yin *et al.* (2023), a system for evaluating the quality of cloud service composition is being created, including the degree of service compliance, composition synergy, and other metrics such as service time, cost, and reliability. A two-criterion composition selection model is then created, which is solved by an improved ant colony algorithm. It can be concluded that both studies describe services in cloud environments using different building blocks. However, the criteria for comparative analysis differ, as this study uses call time and quality, resource usage and scalability, network latency and bandwidth, and another – the degree of compliance and synergy of service composition, service time and cost, and reliability.

Z. Hou *et al.* (2023) explore the session initiation protocol (SIP), which is one of the most popular multimedia communication protocols and has many interesting features, such as advanced and open communication. However, with the rapid development of this protocol, load-balancing issues and security risks have become apparent. This study uses sequential process modelling (CSP) to model SIP and the model analysis (PAT) tool to test the internal and secure properties of a given model. The test results show that SIP has a load-balancing problem and cannot guarantee data security in the event of malicious users. Therefore, the authors improved the model by adding a software-defined network (SDN) architecture and an in-process authentication mechanism. Based on the results of the new test, it becomes evident that the improved model can satisfy internal properties and has improved the security of the SIP model. Like this study, the above-mentioned paper focuses on the protocol of initiating sessions and ensuring their security. However, this study uses cloud-based SBC, while another – tools such as CSP, PAT, and SDN.

S. Wang *et al.* (2022) provide a comprehensive overview of analysis and optimisation performance for stochastic cloud service requests. Analysing the main entities and actions in general performance analysis procedures, a general performance analysis model that includes five main characteristics is proposed: query, sequence, queue, distribution, and services. Practical factors of each characteristic are analysed. The authors discuss the impact of each characteristic on optimisation goals, including costs, profit, response time, and energy consumption. Both studies focus on analysing and optimising service on cloud platforms. However, unlike this study, the 2022 study does not use session initiation protocol trunking and cloud-based session boundary controllers.

In turn, V. Kumar and O. Roy (2020) review security issues in the VoIP voice internet protocol system and reviews several security attacks. For communication between nodes in a VoIP network, a SIP signal protocol is used. The authors continue to review all issues that have a substantial impact on VoIP security and issues, such as data manipulation, replacement attacks, power supply, jitter, and latency. Both studies consider the SIP protocol. However, the 2020 study focuses more on protocol security, and this on more – on improving services using these protocols.

Analysing all the listed papers and comparing them with this one, several key aspects that make this study unique and important in the context of research in the field of cloud technologies can be identified. Firstly, this study tried to cover a wider range of aspects related to the quality of services in cloud systems, including performance analysis, optimisation, security, and sustainability. Compared to the individual aspects discussed in other studies, this paper has provided more completeness and depth in understanding problems. Secondly, SIP trunking and cloud session boundary controllers (SBC) were actively used in this study, which can be an important aspect in the context of improving the quality of Service and security of telecommunications technologies on cloud platforms. This allows submitting new solutions and approaches to improve the quality of communication. Thirdly, the study actively discusses methods for optimising the quality of service in cloud systems, considering various factors such as response time, costs, and energy consumption. This can be useful for practical applications and businesses, as improving productivity and reducing costs are always important. Fourthly, the study evaluated security aspects in telecommunications and cloud systems, considering possible attacks and methods for detecting and preventing them. This makes the study more comprehensive in the form of a discussion of security measures. Lastly, this study actively includes comparative analysis with the work of other researchers, which helped identify common aspects and differences in the papers. This provides a deeper understanding of the context and importance of the work. Overall, this study can make an important contribution to improving the listed technologies and the quality of user communication.

CONCLUSIONS

This study was aimed at analysing the performance of SBC clouds, identifying possible limitations, and proposing optimisation strategies to improve the overall performance, reliability, and user experience of SIP trunking services. Performance research and development of optimisation strategies are important aspects when providing SIP trunking services using cloud-based SBC. This subject is quite relevant in the modern telecommunications industry, as it allows increasing the efficiency and scalability of trunking services in cloud environments. It also allows discovering the benefits and solving problems associated with using cloud-based SBC, helping to improve the user experience and ensuring network reliability. In general, cloud-based SBCs are solutions that ensure the security and control of communication flows in VoIP (voicemail over the Internet) networks. Cloud-based SBC allows connecting IP phone networks to various cloud services, and their main goal is to provide reliable, secure, and efficient routing and processing of session traffic in voice and video communication networks that use the SIP protocol.

Certain cloud-based SBCs, which are quite common were used to implement the study. Practical experiments consisted of modelling SIP test sessions, graphs, diagrams, tables, formulae, and a general application. Based on the investigation and its results, recommendations were made for improving the SBC cloud architecture, using optimisation strategies, exploring alternative solutions, expanding research, practical implementation, monitoring, and support. It is worth implementing effective monitoring and logging systems to quickly identify and solve problems. It is important to support users and operators in solving problems and providing the necessary assistance. The results of the study are of practical importance for developers and operators of telecommunications systems and cloud services. The recommendations obtained can be used to improve the efficiency and safety of various systems. Given the complexity and rapid development of technologies, an important aspect is the possibility of further research in this area in according to the dynamics of the emergence of new technologies.

Possible areas of further research and development may consist of expanding the functionality of SBC, data security and protection, the use of artificial intelligence and data analysis, international aspects and global networks, energy efficiency, standardisation and regulation, integration with other technologies. Exploring opportunities to further expand the functionality of cloud-based SBC, such as integration with other cloud services, video traffic analysis, WebRTC support, etc., is necessary.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abdallah, F. (2019). *VoIP security analysis using the ZRTP method in SIP trunking which uses SBC*. Retrieved from https://repository.mercubuana.ac.id/67267/.

[2] Al Saidat, M.R.S. (2019). A design of an enhanced redundant SIP model for securing SIP-based networks. In *16th international conference on computer systems and applications (AICCSA)* (pp. 1-6). Abu Dhabi: IEEE. doi: 10.1109/AICCSA47632.2019.9035304.

[3] Azure & AWS hosted SBC for Microsoft Teams. (n.d.). Retrieved from https://ribboncommunications.com/solutions/enterprise-solutions/microsoft-solutions/azure-aws-hosted-sbc-microsoft-teams.

[4] Bondarchuk, A., & Zhebka, V. (2023). Protection of a heterogeneous telecommunication network from the influence of destabilizing factors. *Telecommunication and Information Technologies*, 78(1), 4-16. doi: 10.31673/2412-4338.2023.010416.

[5] German, P. (2016). The SIP security fallacy. *Network Security*, 2016(6), 18-20. doi: 10.1016/S1353-4858(16)30060-5.

[6] German, P. (2017). Is your Session Border Controller providing a false sense of security? *Network Security*, 2017(1), 14-16. doi: 10.1016/S1353-4858(17)30007-7.

[7] Hou, Z., Jiaqi, Y., Zhu, H., & Chen, N. (2023). Formalization and verification of SIP using CSP. In H. Takizawa, H. Shen, T. Hanawa, P. Hyuk, J. Park, H. Tian & R. Egawa (Eds.), *Parallel and distributed computing, applications and technologies* (pp. 158-171). Cham: Springer. doi: 10.1007/978-3-031-29927-8_13.

[8] Kaul, S., & Jain, A. (2019). Study on the future of enterprise communication by cloud session border controllers (SBC). In G. Singh Tomar, N.S. Chaudhari, J.L.V. Barbosa & M.K. Aghwariya (Eds.), *International conference on intelligent computing and smart communication* (pp. 407-414). Singapore: Springer. doi: 10.1007/978-981-15-0633-8_39.

[9] Kumar, V., & Roy, O. (2020). Security and challenges in voice over internet protocols: A survey. *IOP Conference Series: Materials Science and Engineering*, 1020, article number 012020. doi: 10.1088/1757-899X/1020/1/012020.

[10] Mazharenko, V. (2020). *Study of the peculiarities of the implementation of IP telephony services in Internet resources*. (Master's thesis, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine).

[11] Nakorji, U., Bello-Salau, H., Adedokun, E., Mustafa, M., & Salami, O.W. (2023). Detection and prevention of SIP register injection attack on a VoLTE network. *Journal of Science, Engineering and Technology*, 2(1), 39-44. doi: 10.59568/KJSET-2023-2-1-06.

[12] Praveen, A., Kumar, S., & Rajendran, S. (2022). Automated testing of session border controller in simulated production environment. *International Journal for Research in Applied Science and Engineering Technology*, 10(6), 4608-4614. doi: 10.22214/ijraset.2022.45035.

[13] Romaniuk, P.I. (2023). Cloud technologies: Analysis, perspectives, implementations. *Computer-Integrated Technologies: Education, Science, Production*, 50, 108-113 doi: 10.36910/6775-2524-0560-2023-50-16.

[14] Skulysh, M., Romanov, O., & Globa, L. (2018). Principle of flows service in the heterogeneous telecommunication environment. *Academic Notes of TNU named after V.I. Vernadskyi*, 29(2), 92-97.

[15] Smirnova, T., Motorin, Y., Buravchenko, K., Bochulia, T., & Kovalenko, O. (2022). Selection of optimal technology of construction of cloud information and communication system of automation of production processes. *Measuring and Computing Devices in Technological Processes*, 1, 15-26. doi: 10.31891/2219-9365-2022-69-1-3.

[16] Tardaskina, T.M., & Hryshchuk, T.V. (2021). Features of use and development of cloud technologies in the digital economy. Biznesinform, 3, 254-260. doi: 10.32983/2222-4459-2021-3-254-260.

[17] Tas, I., Unsalver, B., & Baktir, S. (2020). A novel SIP based distributed reflection denial-of-service attack and an effective defense mechanism. *IEEE Access*, 8, 112574-112584. doi: 10.1109/ACCESS.2020.3001688.

[18] Tokar, L. (2022). Features of building virtual PBX. *Radiotekhnika*, 1(208), 55-64. doi: 10.30837/rt.2022.1.208.06.
[19] Wang, S., Li, X., Sheng, Q., & Beheshti, A. (2022). Performance analysis and optimization on scheduling stochastic cloud service requests: A survey. *IEEE Transactions on Network and Service Management*, 19(3), 3587-3602. doi: 10.1109/TNSM.2022.3181145.
[20] What is a Session Border Controller (SBC)? (n.d.). Retrieved from https://ribboncommunications.com/company/get-help/glossary/session-border-controller-sbc.
[21] Yin, C., Li, S., & Li, X. (2023). A matching-synergy degree-based optimization selection method for cloud manufacturing service composition. *The International Journal of Advanced Manufacturing Technology*. doi: 10.21203/rs.3.rs-2566065/v1.

Покращення надання послуг sip-транкінг за допомогою хмарних SBC: аналіз продуктивності та стратегії оптимізації

Олександр Іванович Підпалий

Аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, пр. Берестейський, 37, м. Київ, Україна
https://orcid.org/0009-0007-6852-7959

Анотація. У сучасних телекомунікаційних мережах транкінг протоколу ініціації сесій є важливою технологією для голосових та відеокомунікацій через мережі Інтернет-протоколу. Хмарні контролери кордонів сесій грають ключову роль у забезпеченні безпеки та якості обслуговування, але виникають виклики щодо їхньої продуктивності та оптимізації, особливо при зростанні обсягу даних та користувачів. Метою статті є розроблення стратегії для досягнення ефективних та масштабованих послуг транкінгу протоколу ініціації сесій в хмарних середовищах. Були використані методи теоретичного аналізу та практичних експериментів. Аналіз продуктивності хмарних контролерів розкрив важливі аналітичні висновки стосовно їх можливостей, а розроблені стратегії оптимізації надали практичні рекомендації для поліпшення надання послуг хмарного транкінгу. Даний аналіз також показав, що продуктивність може варіюватися в залежності від реалізації та налаштувань. Виявлено, що основними факторами, що впливають на продуктивність, є мережева латентність, пропускна спроможність та конфігураційні особливості контролерів. На основі цих відомостей, розроблено стратегію оптимізації, включаючи реалізацію якості обслуговування для пріоритизації трафіку протоколу ініціації сесій, методи автоматичного масштабування ресурсів, резервування та оптимізацію мережевих протоколів. Було продемонстровано, що використання Session Initiation Protocol-транкінгу та хмарних Session Border Controller може значно покращити якість обслуговування в телекомунікаційних системах, що дає можливість оптимізувати маршрутизацію дзвінків та забезпечити безпеку комунікацій. Оцінка продуктивності хмарних Session Border Controller надала цінне уявлення про їхні можливості, а пропоновані стратегії оптимізації можуть стати конкретними рекомендаціями для поліпшення надання послуг Session Initiation Protocol-транкінгу в хмарних середовищах. Результати дослідження можуть служити цінними рекомендаціями для фахівців у галузі телекомунікацій, які прагнуть розгортати ефективні та масштабовані рішення транкінгу в хмарних мережах

Ключові слова: протокол ініціації сесій; якість обслуговування комунікацій; контролери кордонів сесій; мережеві затримки; скалабельність ресурсів