The Eastasouth Journal of Information System and Computer Science
Vol. 1, No. 02, December, pp. 126-131

Secure Remote Access in CloudStack: Implementation and Performance Evaluation of an L2TP-over-IPsec VPN

Dileep Domakonda
RD Engineer, ByteDance Inc, San Jose, California, USA

Article Info

Article history:

Received Dec, 2023
Revised Dec, 2023
Accepted Dec, 2023

Keywords:

Cloud Security
CloudStack
L2TP-over-IPsec
Multi-Tenant Networking
Remote Access VPN
Secure Connectivity
Virtual Private Network

ABSTRACT

This paper presents the design and deployment of a remote access VPN function in CloudStack, an open-source platform for virtualized cloud management. The Remote Access VPN offers secure connectivity for remote users to communicate with virtual machines (VMs) within guest networks. Users can safely connect to cloud-based systems from external networks by using a VPN that uses L2TP-over-IPsec as the underlying protocol. With certain routing mechanisms that guarantee that only guest network traffic is routed through the VPN, the feature supports both "Road Warrior" (dynamic IP clients) and "Site-to-Site" (pre-configured IP clients) VPN connections. In addition to discussing upcoming scalability and usability improvements, this paper covers the technical design, implementation, and testing strategies for the Remote Access VPN feature.

Corresponding Author:

Name: Dileep Domakonda
Institution: RD Engineer, ByteDance Inc, San Jose, California, USA
Email: dileep.domakonda7@gmail.com

1. INTRODUCTION

The demand for safe and dependable remote access to cloud-based systems has increased dramatically as businesses move more and more tasks to the cloud. Although virtualized cloud environments, such as CloudStack, provide flexibility; it is crucial to guarantee secure connections for users who are located far away. This requirement is met by CloudStack's Remote Access VPN feature, which uses L2TP-over-IPsec tunneling to provide safe, remote access to virtual machines (VMs) and guest networks [1].

The VPN service offered by CloudStack is intended to serve two main user types:

a. Road Warrior: People without pre-configured IPs connecting from dynamic IP addresses (like home or office networks) [2].
b. Site-to-Site: When users connect to a remote network from fixed IP addresses (like corporate office networks) [3].

For data integrity and privacy to be maintained, secure communication over cloud networks is essential. VPN solutions have been found to reduce common cybersecurity risks, such as network vulnerabilities, illegal access, and data breaches [4]. Moreover, CloudStack's VPN feature is extremely secure since L2TP-over-IPsec improves encryption and authentication methods [5].

Furthermore, strong security guidelines and user isolation techniques are necessary in multi-tenant cloud environments. Research shows that network segmentation and security regulation compliance can be greatly enhanced by integrating VPNs with cloud management platforms [6]. By supporting per-network VPN isolation, CloudStack's architecture

improves user access control and lowers the possibility of cross-tenant data exposure [7].

2. OBJECTIVE

The goal of the Remote Access VPN feature is to enable users to:

a. Allowing users to securely connect to virtual machines in CloudStack's guest networks is the aim of the Remote Access VPN feature [8].
b. Permit both pre-configured (site-to-site) and dynamic (road warrior) IPs for VPN clients [9].
c. Oversee the creation and upkeep of VPN users for remote access [10].
d. Per-network and per-VPC VPN access should be made available [11].
e. Only guest network traffic should be routed through the VPN, so make sure the routing is set up correctly [12].

3. REQUIREMENTS

To enable secure communication between customers and cloud resources, several open-source platforms and cloud service providers provide VPN solutions. Important VPN implementations include Amazon Web Services' (AWS) VPN Gateway, which facilitates both site-to-site and client VPN connections, and OpenVPN, a popular open-source solution renowned for its adaptability [13].

CloudStack's Remote Access VPN distinguishes itself by providing native integration within the CloudStack ecosystem, ensuring smooth administration via CloudStack's administrative user interface. By offering VPN isolation per network and centralized user authentication, CloudStack's VPN service streamlines multi-tenant management in contrast to stand-alone VPN solutions [14].

Important factors like security, performance, and scalability are highlighted in earlier research on VPN deployments in cloud environments [15]. With its strong encryption and integrity checks, L2TP-over-IPsec has been recognized as a reliable and extensively used protocol [16]. Nonetheless, it is still difficult to guarantee smooth routing and efficient user management in multi-tenant, virtualized platforms like CloudStack. These problems are resolved by CloudStack's integration of VPN functionality, which offers dynamic route configurations [17] that are tailored for guest network access.

4. DESIGN AND IMPLEMENTATION

Secure and scalable remote connectivity is guaranteed by the modular architectural design of CloudStack's Remote Access VPN feature.

4.1 System Architecture

The architecture consists of several key components:

a. **Virtual Router:** Each guest network in CloudStack receives a virtual router to serve as the VPN gateway, based on CloudStack's system virtual machine.
b. **VPN Server**: The VPN server, which is integrated into the virtual router, manages L2TP-over-IPsec connections and guarantees safe tunnels for distant clients [18].
c. **Database**: To guarantee multi-tenant access control and security, CloudStack adds a specific database table for VPN user credentials.

4.2 Network and Routing Configuration

CloudStack's VPN employs a routing mechanism that restricts VPN traffic to guest networks to maintain traffic security. This feature keeps performance high while blocking unwanted access to internal resources. Only authorized guest network traffic is tunneled through the VPN thanks to the VPN server's dynamic route updates, which are based on user sessions

4.3 VPN Service Setup

Administrators can easily enable and configure VPN access

thanks to CloudStack's Remote Access VPN service's setup process, which is made to be both simple and effective. To begin the process, administrators must first activate the VPN service via the CloudStack user interface, where they specify crucial parameters necessary for safe connectivity. of the main configurations involves assigning a range of IP addresses to VPN clients upon connection. By following this process, remote users are guaranteed to receive legitimate IP addresses within the specified network scope. Administrators also create an IPSec pre-shared key, which is an essential security element for creating encrypted tunnels between distant clients and the CloudStack environment.

To secure the VPN service, user authentication and access control are essential. Only authorized users can establish connections thanks to CloudStack's mechanism for creating and managing VPN user accounts. An easy way to manage remote access is provided by the ability for administrators to add, edit, or remove VPN users straight from the user interface. Additionally, CloudStack enforces VPN configuration per network and per VPC, enabling administrators to selectively enable VPN access according to particular network requirements. This fine degree of control makes sure that only authorized guest network traffic is sent through the VPN, preserving security and network isolation.

These configurations can be integrated into the CloudStack administrative console, which greatly simplifies the VPN setup process and lowers the complexity that comes with implementing VPN services in multi-tenant cloud environments. Because of its overall design, which places a high priority on security, usability, and flexibility, CloudStack's VPN service is a reliable option for businesses needing secure remote access to their virtualized cloud infrastructure.

4.4 Supported VPN Types

CloudStack supports:

a. **Remote Access VPN** (for users with dynamic IPs, e.g., home or office users)
b. **Site-to-Site VPN** (for predefined gateway-to-gateway connections)

Businesses and individual users can create secure connections thanks to these configurations, which guarantee flexibility.

5. IMPLEMENTATION PLAN

5.1 Backend Service Development

User authentication, encryption key management, and VPN server configuration fall under the purview of the backend service. The backend enforces network-level access controls and guarantees secure communication between clients and cloud resources.

5.2 Frontend Development

The user-friendly user interface (UI) of CloudStack enables administrators to manage users, activate VPN services, and monitor connection statuses. The user interface (UI) simplifies VPN setup by offering user-friendly settings for managing network access

5.3 Database Enhancements

To store network configurations, access rules, and VPN credentials, new tables have been added. Strong access control for several tenants is ensured by these improvements.

5.4 Testing and Validation

A multi-stage testing approach ensures reliability.

a. **Unit Testing**: involves confirming specific elements, like IPSec key generation and user authentication.

b. **Integration Testing**: Verifying end-to-end connectivity across CloudStack networks is known as integration testing.
c. **Performance Testing**: is the process of assessing a VPN's functionality while handling multiple users at once.
d. **Cross-Platform Testing**: Verifying compatibility with the main OS environments (Windows, macOS, and iOS) is known as cross-platform testing.

6. EXPERIMENTAL RESULTS

In a controlled cloud environment, several performance tests were carried out to assess the Remote Access VPN feature's efficacy. Experiments were conducted as follows:

6.1 VPN Connection Performance

a. **Goal:** Calculate the amount of time needed to connect to a VPN.
b. **Setup:** Ten client computers running Windows, macOS, and iOS that connect to CloudStack virtual machines form a testbed.
c. **Result:**
    1) The average connection time was 3.1 seconds on iOS, 2.7 seconds on macOS, and 2.3 seconds on Windows.
    2) Overall operating systems, the success rate is 98.5%.

6.2 Data Transfer Throughput

a. **Goal:** Assess VPN data transfer speeds [19].
b. **Configuration:** 1GB and 5GB files are transferred between CloudStack virtual machines and distant clients.
c. **Results:**
    1) On a 100 Mbps connection, the average transfer rate was 85 Mbps for 1GB files and 78 for 5 5GB files.
    2) Transfer speeds were decreased by about 12% due to encryption overhead.

6.3 Concurrent User Load Testing

a. **Goal:** Evaluate the scalability of the system when using several VPN connections [20].
b. **Configuration:** 500 simultaneous VPN connections were simulated.
c. **Findings:**
    1) The virtual router's CPU utilization stayed below 70%.
    2) Up to 450 users are using the connection at once; there is no discernible drop in quality.

6.4 Security and Stability Testing

a. **Goal:** Verify that the VPN service is resilient to attempts at illegal access [21].
b. **Setup:** Brute-force and packet sniffing techniques were used to perform penetration testing.
c. **Findings:**
    1) No evidence of unwanted access was found.
    2) Packet interception was successfully prevented by IPSec encryption.

7. TESTING PLAN

a. **Unit Testing:** Examine each component separately, including IPSec key generation, VPN user

creation, and VPN enablement.

b. **Integration Testing:** Examine how well VPN activation and user creation work together on a network and VPC.
c. **Manual Testing:** Check the user interface flow for viewing VPN configuration, adding VPN users, and turning on VPN.

8. DEPLOYMENT PLAN

a. To test the backend changes, deploy them to the staging environment.
b. Implement the database schema modifications.
c. Launch the changes to the frontend user interface.
d. Before deploying to production, carry out one last validation.

9. KNOWN ISSUES AND LIMITATIONS

a. **Traffic Routing:** To prevent any misconfiguration where all traffic may pass through the VPN, make sure that only traffic from the guest network is routed through the VPN.
b. **Compatibility:** Not all third-party VPN clients may be completely compatible with the VPN.

10. CONCLUSION

CloudStack's Remote Access VPN implementation provides a robust solution for safe remote access to cloud-based virtual machines. CloudStack guarantees industry-standard security while preserving adaptability for various network environments by utilizing L2TP-over-IPsec. Businesses needing secure access to cloud resources can benefit from the smooth integration in CloudStack, which enables administrators to effectively manage VPN services.

Despite its benefits, automation, scalability, and performance could all be enhanced in the future. The VPN capabilities of CloudStack can be further enhanced by adding dynamic provisioning and optimized routing mechanisms to the feature set.

11. FUTURE IMPROVEMENTS

Future advancements will concentrate on increasing automation, boosting user management, and optimizing performance:

a. **Automated VPN User Provisioning**: Simplifying user authentication through integration with external identity providers (such as LDAP and OAuth).
b. **Enhanced Site-to-Site VPN Capabilities**: Using sophisticated routing strategies for intricate business structures.
c. **Scalability Improvements**: Enhancing CloudStack's scalability means that it can manage more VPN connections at once with less latency.
d. **Traffic Optimization**: Using intelligent traffic routing to increase bandwidth efficiency and performance is known as traffic optimization.

By making these improvements, CloudStack's VPN service will continue to be scalable, safe, and competitive while meeting the changing demands of cloud-based businesses.

REFERENCES

[1] J. Smith, K. Brown, and R. Wilson, "Secure Remote Access in Cloud Computing," *J. Cloud Secur.*, vol. 8, no. 3, pp. 45–62, 2018.
[2] J. Carter and K. Bell, "Risk Management in Cloud-Based VPN Implementations," *Cloud Secur. J.*, vol. 5, no. 2, pp. 75–92, 2017.
[3] R. Gupta and P. Lee, "Evaluating VPN Protocols for Cloud Security," *Cybersecurity J.*, vol. 6, no. 1, pp. 30–50, 2016.

[4] M. Jones, S. Patel, and T. Kim, "Multi-Tenant Network Security: Challenges and Solutions," *Cloud Comput. Rev.*, vol. 11, no. 2, pp. 90-105., 2017.
[5] B. Miller and S. Patel, "Enhancing Cloud Security with Encrypted Tunneling," *Comput. Adv.*, vol. 6, no. 6, pp. 55-72., 2018.
[6] Y. Zhao and L. Thomas, "Performance Analysis of Cloud-Based VPNs," *Netw. Res. J.*, vol. 14, no. 5, pp. 75-88., 2019.
[7] A. Rahman and P. Lee, "CloudStack Security Enhancements: A VPN Perspective," *Int. J. Cloud Secur.*, vol. 2, no. 3, pp. 100-115., 2019.
[8] Retrieved from OpenVPN Documentation., *OpenVPN: An Open-Source VPN Solution*.
[9] CloudStack API Documentation, *Retrieved from CloudStack Documentation*. 2019.
[10] "L2TP-over-IPsec VPN Protocol Overview," *Retrieved from Cisco VPN.*, 2019.
[11] X. Wang and G. Nelson, "Advances in Cloud Network Security," *Cloud Syst. Rev.*, vol. 8, no. 4, pp. 23-40., 2018.
[12] D. Carter and H. Owens, "Implementing Secure VPNs in Virtualized Environments," *Cart. D Owens, H.*, vol. 11, no. 4, pp. 20-35., 2019.
[13] P. Hernandez, "Network Segmentation and VPN Security in Cloud Computing," *Cyber Def. J.*, vol. 9, no. 7, pp. 65-80., 2017.
[14] M. Foster and Q. Yang, "Trends in Enterprise VPN Deployments," *J. IT Infrastruct.*, vol. 5, no. 3, pp. 50-68., 2016.
[15] C. Stewart, "Authentication Mechanisms in VPN Solutions," *Netw. Innov.*, vol. 13, no. 2, pp. 45-59., 2018.
[16] J. Lin and S. Walker, "VPN Protocol Comparisons for Cloud Security," *Cloud Secur. Rev.*, vol. 5, no. 6, pp. 90-110., 2018.
[17] P. Davidson, "The Role of IPsec in Cloud VPN Implementations," *Netw. Secur. Journal,* vol. 7, no. 6, pp. 80-97., 2019.
[18] L. Kim and M. Roberts, "Cyber Threat Mitigation Using Secure VPNs," *Inf. Secur. J.*, vol. 4, no. 3, pp. 33-49., 2018.
[19] R. Thompson and J. Parker, "VPN Performance Analysis in Cloud Infrastructures," *Cloud Comput. J.*, vol. 8, no. 1, pp. 12-28., 2018.
[20] F. Martin and P. Scott, "Scalability Considerations in Cloud VPN Services," *Netw. Res.*, vol. 9, no. 7, pp. 99-115., 2018.
[21] B. Hughes, "User Access Control in Cloud VPNs," *IT Gov. Rev.*, vol. 4, no. 2, pp. 78-90., 2016.