

CASE STUDY

Implementing a Robust VPN Solution for Secure Remote Access to Cloud Resources

Presented By.

<u>Name</u>	<u>Registration No.</u>
1. Ankit Kumar Panda	2241016052
2. Piyush Kumar Sahoo	2241019096
3. Barun Kumar Rout	2241018145





TABLE OF CONTENTS

SL. NO.	TITLE
1	INTRODUCTION
2	MOTIVATION
3	WITHOUT VPN VS WITH VPN
4	SOLUTION DEVELOPMENT
5	IMPLEMENTATION
6	RESULT
7	CONCLUSION
8	REFERENCES

INTRODUCTION

- Organizations increasingly depend on cloud resources (AWS EC2, RDS, etc.)
- Remote work culture requires employees to access cloud services from anywhere.
- Directly exposing resources to the internet leads to security threats.
- A VPN solution allows secure and private connectivity to AWS VPC resources.
- This project focuses on AWS Client VPN with IAM authentication to provide safe and scalable access.



MOTIVATION

- Protect sensitive business data from cyberattacks and unauthorized access.
- Provide remote teams with seamless and secure connectivity.
- Eliminate risks of public-facing SSH/RDP connections.
- Reduce operational complexity with IAM-based authentication.
- Ensure the solution is robust, scalable, and easy to manage for future needs.



WITHOUT VPN VS WITH VPN

Without VPN:

- Data travels in plaintext over the internet.
- Easy for attackers to sniff/modify traffic.
- No identity verification of users.



With VPN:

- Data is encrypted using protocols (AES, IPsec).
- Private tunnel → only authenticated users connect.
- Cloud resources hidden from direct internet exposure.
- Strong authentication: Certificates, IAM, MFA.





SOLUTION DEVELOPMENT

Our proposed VPN solution integrates modern security protocols and architectures:

- Site-to-Site VPN for organization-to-cloud secure link. (IKEv2 + IPsec)
- Point-to-Site VPN for individual remote user access.
- Robust Authentication & Key Exchange (OpenVPN, Certificates, MFA).



SOLUTION DEVELOPMENT

Site-to-Site VPN Architecture:

Use Case:

Connects an organization's on-premises data center securely with cloud VPC.

How it works:

- A VPN gateway (router/firewall) at each site.
- Tunnels established via Ipsec+IKEv2.
- Encrypted communication between data center and cloud resources.

Advantages:

- Permanent connection.
- Best for multiple users in branch offices.

SOLUTION DEVELOPMENT

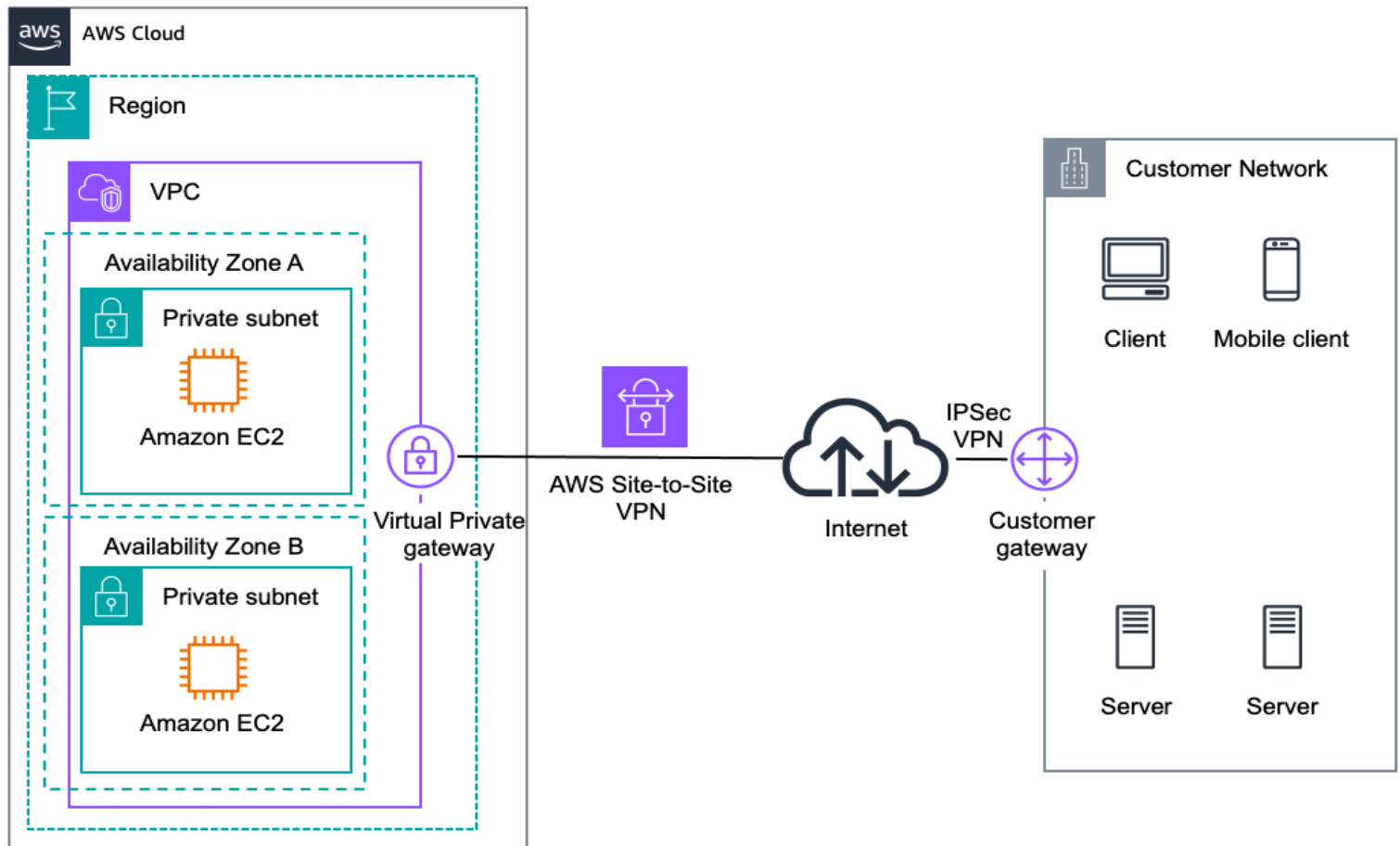


Fig : Site-To-Site VPN Architecture



SOLUTION DEVELOPMENT

Point-to-Site VPN Architecture:

Use Case:

Individual employees working remotely.

How it works:

- User installs VPN client on laptop/phone.
- Client authenticates via certificate / username-password + MFA.
- Secure tunnel established directly to Cloud VPN gateway.

Advantages:

- Flexible – works from anywhere.
- Best for small teams or remote users.

SOLUTION DEVELOPMENT

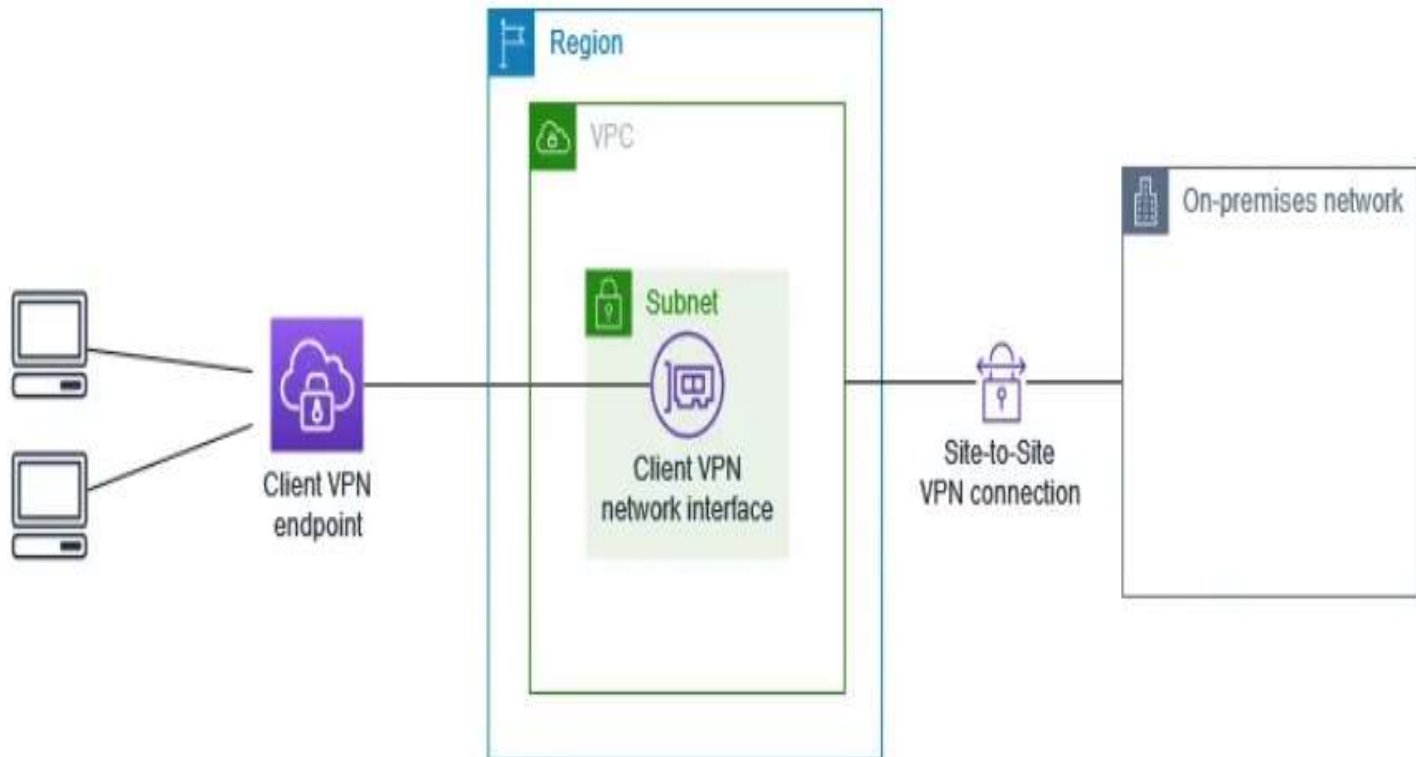


Fig : Point-To-Site VPN Architecture

SOLUTION DEVELOPMENT

Authentication & Key Management :

Key Exchange (TLS Handshake):

- Uses OpenVPN (TLS/SSL) for secure tunneling.
- Diffie–Hellman ensures unique keys per session.

Authentication Mechanisms:

- Using Digital Certificates: Each client and server has its own certificate issued by a trusted CA.
- Certificates validate identities.

Multi-Factor Authentication Integration Session Security:

- Perfect Forward Secrecy (PFS) ensures new keys per session(Uses Diffie–Hellman).
- Even if one session key is compromised, past/future sessions remain safe.



IMPLEMENTATION

Step 1: Set Up VPC, Subnets, and Route Tables.

VPC (VPN): (10.0.0.0/16)

Creating Subnets:-

Public Subnet (PUB): 10.0.1.0/24

Private Subnet (PVT): 10.0.2.0/24

Creating Internet Gateway:-

Internet Gateway (IGW): VPN-IGW

Creating Route Table:-

Public Route Table (PUB-RT)

Private Route Table (PVT-RT)

Creating Associations:-

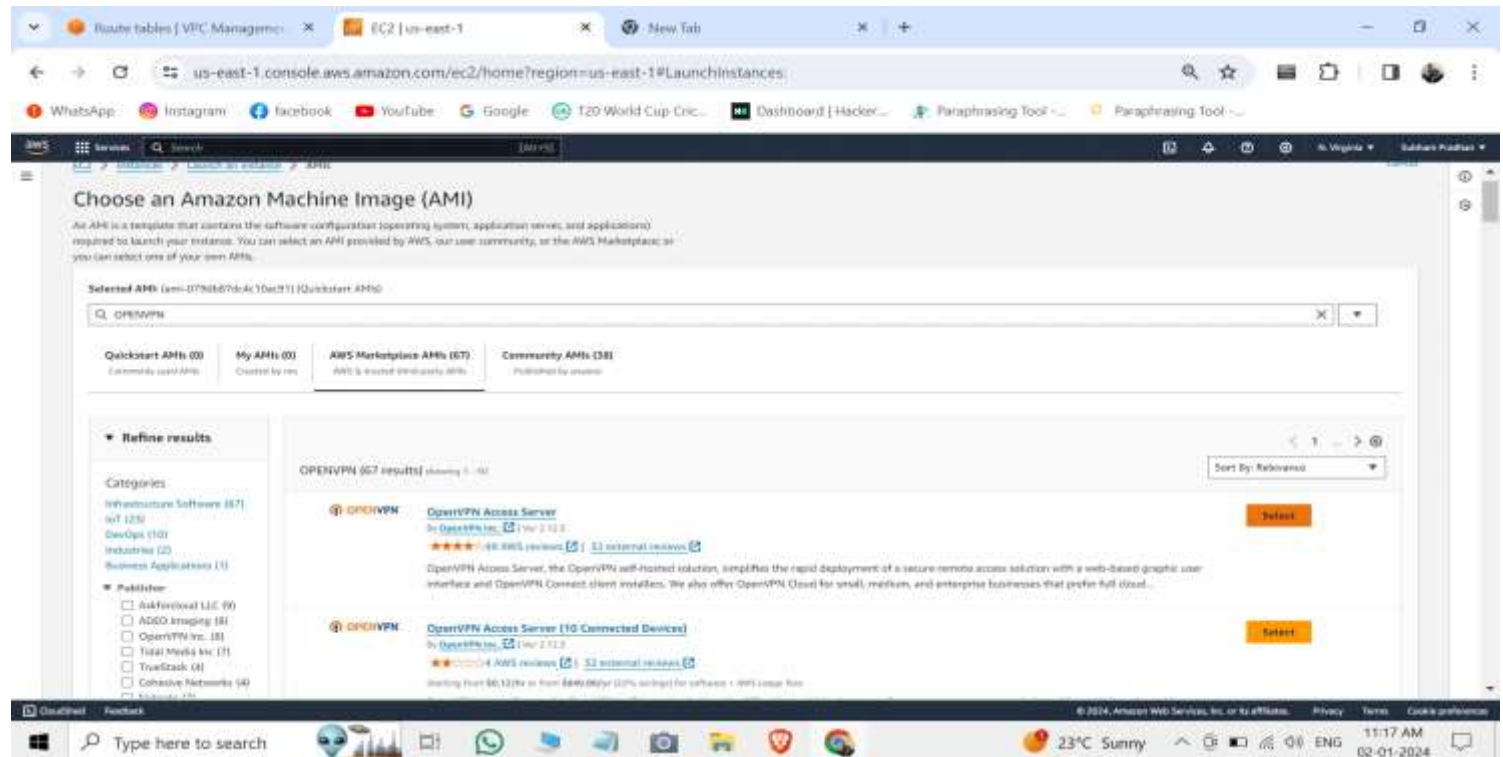
Associate IGW and PUB-RT with the PUB subnet

Associate PVT-RT with the PVT subnet

IMPLEMENTATION

Step 2: Launch OpenVPN Server

Launch an EC2 instance named “OPENVPN” using the OpenVPN AMI.



- Set a password for the OpenVPN Admin UI and Client UI.
- Copy the Admin UI and Client UI.

IMPLEMENTATION

Step 2: Launch OpenVPN Server

```
openvpnas@ip-10-0-1-32: ~  
Adding web group...  
groupadd: group 'openvpn_as' already exists  
Adjusting license directory ownership...  
Initializing confdb...  
Initial version is not set. Setting it to 2.12.3...  
Generating PAM config for openvpnas ...  
Enabling service  
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service -> /lib/systemd/system/openvpnas.service  
Starting openvpnas...  
  
NOTE: Your system clock must be correct for OpenVPN Access Server  
to perform correctly. Please ensure that your time and date  
are correct on this system.  
  
Initial Configuration Complete!  
  
You can now continue configuring OpenVPN Access Server by  
directing your Web browser to this URL:  
  
https://34.237.245.104:943/admin  
  
During normal operation, OpenVPN AS can be accessed via these URLs:  
Admin UI: https://34.237.245.104:943/admin  
Client UI: https://34.237.245.104:943/  
To login please use the "openvpn" account with the password you specified during the setup.  
  
See the Release Notes for this release at:  
https://openvpn.net/vpn-server-resources/release-notes/  
  
openvpnas@ip-10-0-1-32:~$ |
```


IMPLEMENTATION

Step 3: Connect to Admin UI

The image displays two screenshots of the OpenVPN Access Server Admin UI. The top screenshot shows the 'Admin Login' page with the OpenVPN logo and a login form. The bottom screenshot shows the 'User Permissions' page with a sidebar menu and a table of users.

Admin Login Page:

OpenVPN Access Server

Admin Login

Username: openvpn

Password: [Redacted]

Sign In

POWERED BY OPENVPN © 2008-2023 OpenVPN Inc. All Rights Reserved

User Permissions Page:

OpenVPN Access Server v2.10.2

STATUS

CONFIGURATION

USER MANAGEMENT

Authentication

Tools

Documentation

User Permissions

User Profiles

Group

Permissions

Search By Username/Group (use % as wildcard)

No Default Group

Search/Refresh

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group	[Edit]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
New Username	No Default Group	[Edit]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Settings

Type here to search

23°C

11:35 AM 02-01-2024

IMPLEMENTATION

Step 4: Connect to Client UI & Download Connection Profile

- Connect to the Client UI.
- Install the OpenVPN client app on your device.
- Download the connection profile from the Client UI.



IMPLEMENTATION

Step 4: Connect to Client UI & Download Connection Profile



IMPLEMENTATION

Step 5: Test VPN Connection

- Ping the Private IP of the OpenVPN server; it will not work.

```
MINGW64/c/Users/ASUS/Downloads
ASUS@LAPTOP-Q9QDRNKO MINGW64 ~/Downloads
$ ping 10.0.1.32

Pinging 10.0.1.32 with 32 bytes of data:
Request timed out.
Request timed out.
```

- Log in using the user ID and password in the OpenVPN client.
- Upload the downloaded profile file then connect.



IMPLEMENTATION

Step 5: Test VPN Connection

- Ping again

```
ASUS@LAPTOP-Q9QDRNKO MINGW64 ~/Downloads
$ ping 10.0.1.32

Pinging 10.0.1.32 with 32 bytes of data:
Reply from 10.0.1.32: bytes=32 time=272ms TTL=64
Reply from 10.0.1.32: bytes=32 time=322ms TTL=64
Reply from 10.0.1.32: bytes=32 time=394ms TTL=64
Reply from 10.0.1.32: bytes=32 time=424ms TTL=64

Ping statistics for 10.0.1.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 272ms, Maximum = 424ms, Average = 353ms
```


-



IMPLEMENTATION

Step 7: Test Communication with NAT Gateway

- Reconnect to the OpenVPN server.
- Ping the private IP of the APP-SERVER; it should ping due to the NAT Gateway.

```
openvpnas@ip-10-0-1-32:~$ sudo su
root@ip-10-0-1-32:/home/openvpnas# ping 10.0.1.32
PING 10.0.1.32 (10.0.1.32) 56(84) bytes of data:
64 bytes from 10.0.1.32: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 10.0.1.32: icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from 10.0.1.32: icmp_seq=3 ttl=64 time=0.048 ms
64 bytes from 10.0.1.32: icmp_seq=4 ttl=64 time=0.045 ms
64 bytes from 10.0.1.32: icmp_seq=5 ttl=64 time=0.046 ms
64 bytes from 10.0.1.32: icmp_seq=6 ttl=64 time=0.049 ms
64 bytes from 10.0.1.32: icmp_seq=7 ttl=64 time=0.044 ms
```

- Create a test-key on APP-SERVER, change permissions, and perform an SSH connection.

```
root@ip-10-0-1-32:/home/openvpnas#
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAj6n3FzV46N0y2b30K5F1KV4b3N8duxuSkNoGNCBNRoOALzX8
bG4uYzLaL F7KLF513hd/1TTr1d7GwCCUgmj39G6vATNwwa6X33M5oC9N3IfGe0pw
jHza+671A1Zw9IK8XN/N9z9A1n05o0hsV7HZIL7wCn+ZpQTGN1T5XxS0tELbiqk
duNUGTcOoBok1cterS85btLrq04nhwitUyrmUExqNRkOP59fi5cdy0ekUxg1DH2h0
xgE1BVuZ+yuRIDj902wTos8IcoelbFCNDX8S90b+a1r/QyKfLFgKv511y5TprJRk
jXu0s3426Ak41d1/A014b55LS+HvETdIugp+xQIDAQABAQIBAEPIurdwqyf15npk
YAy2egRevPLH6wNpNMxXspmhRBRBM34TENjww736F1uhj17FEgoJJC54w9X7WMZ4
CNpHqmb5+mSsnocgKF2Zj1VOPGqTP2kq1FQvDRW3h59f98j7oGIwRpRLFq2nWB/3
8y/HMn1AO+trVPd9Yk1VLXqX4FRLTMVOIjaoqcbh+wPY3cs+Dp5IR0WENS42GnKE
G5tGdgkcNxFF5Q6QaEomVxxA9UsfYJm1InpZYAvswH8DQ6HPh1RZZ3kzj6DUiBo
etGbDbUDM51rZPp7D4VtrZ1v/pvTmboxh3GrqaxU2Z23jVQaat40ZHEykaoBUXDU
I+P+6vkCgYEAYo15a1v351TVbnPFGxN3PSYveQQ3YrtCAd93ssvhj428nr5+rmJO
5Fh3uybkWZS9M25WLVJmtvyL1hd1FmknbpVwF2J9QsTPgZ2H1ZM1rezgAsXxREKA
VHI7Xucx2b4w/qbNfKukyTQxz+tmDkw8hCkhrhDowplGTIm10y/s1s8CgyEAtZ3u
qs3HC/ssC6A2HECM/e/et4b5NmdXHuDorF505FKuc2j3LuARdwFV16tEqvbk6tEr
eTjoGEj6ye6OowPA/PD1ks86d/CdjpLRUyDzkrp+wZM8ADLR/qL0OrxHKEo/Tb3B
5GD6WEDfqn1bpvBFTpFAZtUB+634k1coiGRUNisCgYAgRQPH53NB57b5H9+snBM
zvQ3Onw8dA8HeVuvj43C+hjH2z+PF8GGXZXNqjNorCqsIgamt88Hbhq1JAqLexs/
wvIcV6XfIk3Q35EjDKT3Hzretjxm3jVnxRehNbt6bjOODnLOD18ucwksJduwExs9
OvR/r8/kx1eEEbn1ysXXwK8gEMQ712wyywk11UH/VUqLHfTeOrmsQB77pmSO38H
eKerPpSUbDbpLFPp11BwPq0jhxS50znXsxQaj6u6bMySjklLV5S8BnmNrDshvB
BRXosm8vwhbuRgoeaJWwV7cvDYjakVaY139nnvVQK8FSuFbX4fDZttzOmQV2qT1p
dq13AoGBAIfmPABChmNZ4wkNjtwxwBH6kDH17g/uowjAHBzXKwSUKSto1G21+xH
K9Mm5og5SgM1mUH7KbDsIU3P/IbHy1Qc+oMDvNoSbd4LrusfNwt4DhdJGHHT7FqQ
XH1/iUPBhOrvkZ92j6F5TdRayhgOXIJz8b2emS2d+PyjdGpvjUXv
-----END RSA PRIVATE KEY-----

-- INSERT --
```



```
[ec2-user@ip-10-0-2-248 ~]$ ping google.com
PING google.com (172.253.62.101) 56(84) bytes of data:
64 bytes from bc-in-f101.1e100.net (172.253.62.101): icmp_seq=1 ttl=104 time=2.60 ms
64 bytes from bc-in-f101.1e100.net (172.253.62.101): icmp_seq=2 ttl=104 time=1.85 ms
64 bytes from bc-in-f101.1e100.net (172.253.62.101): icmp_seq=3 ttl=104 time=1.90 ms
64 bytes from bc-in-f101.1e100.net (172.253.62.101): icmp_seq=4 ttl=104 time=1.84 ms
64 bytes from bc-in-f101.1e100.net (172.253.62.101): icmp_seq=5 ttl=104 time=1.88 ms
64 bytes from bc-in-f101.1e100.net (172.253.62.101): icmp_seq=6 ttl=104 time=1.86 ms
```

IMPLEMENTATION

Step 8: Install Apache Server on APP-SERVER

- Switch to sudo su on APP-SERVER.
- Install Apache: `yum install httpd -y`.
- Start Apache: `systemctl start httpd`.
- Check status: `systemctl status httpd`.

```
root@ip-10-0-2-248:/home/ec2-user
Installed:
  httpd.x86_64 0:2.4.58-1.amzn2

Dependency Installed:
  apr.x86_64 0:1.7.2-1.amzn2
  apr-util-bdb.x86_64 0:1.6.3-1.amzn2.0.1
  httpd-filesystem.noarch 0:2.4.58-1.amzn2
  mailcap.noarch 0:2.1.41-2.amzn2
  apr-util.x86_64 0:1.6.3-1.amzn2.0.1
  generic-logos-httpd.noarch 0:18.0.0-4.amzn2
  httpd-tools.x86_64 0:2.4.58-1.amzn2
  mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
[root@ip-10-0-2-248 ec2-user]#
[root@ip-10-0-2-248 ec2-user]#
[root@ip-10-0-2-248 ec2-user]#
[root@ip-10-0-2-248 ec2-user]# systemctl start httpd
[root@ip-10-0-2-248 ec2-user]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-01-02 06:31:39 UTC; 16s ago
     Docs: man:httpd.service(8)
   Main PID: 3458 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
   CGroup: /system.slice/httpd.service
           └─3458 /usr/sbin/httpd -DFOREGROUND
             └─3459 /usr/sbin/httpd -DFOREGROUND
               └─3460 /usr/sbin/httpd -DFOREGROUND
                 └─3461 /usr/sbin/httpd -DFOREGROUND
                   └─3462 /usr/sbin/httpd -DFOREGROUND
                     └─3463 /usr/sbin/httpd -DFOREGROUND

Jan 02 06:31:39 ip-10-0-2-248.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Jan 02 06:31:39 ip-10-0-2-248.ec2.internal systemd[1]: Started The Apache HTTP Server.
[root@ip-10-0-2-248 ec2-user]#
```

RESULT

Access Apache by pasting the private IP of APP-SERVER; it should display the Apache server.

(Note: Ensure that the VPN connection is active during testing.)

The screenshot shows a web browser window with multiple tabs. The active tab is titled 'Test Page for the Apache' and displays a 'Test Page' with a red header. The page content includes instructions for testing the Apache HTTP server and information for general public and website administrators. An OpenVPN Connect overlay is visible on the right side of the browser window, showing a 'CONNECTED' status for the 'OpenVPN Profile' with the email 'openvpn@34.237.245.104'. The overlay also displays 'DISCONNECTED' and 'CONNECTION STATS' with a graph showing data transfer rates. The Windows taskbar is visible at the bottom of the screen.

Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below as a logo for your website.

OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile

openvpn@34.237.245.104
[profile-6898194693460605830]

DISCONNECTED

CONNECTION STATS

4.6KB/s

0B/s

BYTES IN 63 B/S

BYTES OUT 65 B/S

25°C

12:03 PM

02-01-2024

CONCLUSION

- Implemented a secure Point-to-Site VPN using AWS Client VPN service.
- Enabled remote user access to AWS VPC resources via an encrypted, OpenVPN-based tunnel.
- Ensured confidentiality, integrity, and controlled access with mutual TLS authentication and AWS IAM/ACM integration.
- Achieved scalability, flexibility (split-tunnel/full-tunnel), and observability.
- Final outcome: Remote users can securely connect and manage AWS cloud resources as if they were inside the VPC without exposing them directly to the internet.



REFERENCES

- **AWS Documentation – Client VPN**
<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/what-is.html>
- **Medium – Point to Site Connection**
<https://medium.com/@subhampradhan966/setting-up-point-to-site-vpn-connection-in-aws-a-step-by-step-guide-9edd65e6ca44>
- **AWS Documentation – Tutorial: Create and Configure a Client VPN Endpoint**
<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/cvpn-getting-started.html>
- **Nord VPN - What is it, and how does it work?**
<https://nordvpn.com/blog/point-to-site-vpn/?srsltid=AfmBOoruoxZL6qczyCqvfo1h1imnnMaWL4FkDnzhw1AZ2yWUOIRPsyG5>