Expert Cloud Consulting

Enhance Optimise & Scale

ASCP GPUonCLOUD Pvt Ltd

“Expert Cloud Consulting” -

Documentation For Setting Up a Web Server and Client with Private IPs and Secure File Transfer [Title,18, Arial]

14.April.2025 [Subtitle,14, Arial]

version 1.0

—

Contributed by Yogiraj Deshpande [Normal text,14, Arial]
Approved by Akshay Shinde(In Review)
Expert Cloud Consulting
Office #811, Gera Imperium Rise,
Hinjewadi Phase-II Rd, Pune, India – 411057

“Expert Cloud Consulting”
Documentation For Setting Up a Web Server and Client with Private IPs and Secure File Transfer[Title,18, Arial]

1.0: Document Overview:

This document outlines the basic networking topology and secure communication setup between two private VMs. The goal is to configure a web server, establish client connectivity, and enable secure file transfer, even without direct public access to the instances.

2.0: Objective:

- Set up two Linux VMs with private IP addresses only.
- Configure one VM as a Web Server (using Nginx default page).
- Configure the second VM as a Client to access the web server.
- Use SSH and SCP to securely transfer files between VMs.
- Implement bastion host access since the VMs are private.

3.0: Prerequisites:

- Two Linux VMs launched with only private IPs.
- A Bastion Host (Public Linux VM) available.
- Security Groups configured:
  - Bastion allows SSH (port 22) from your IP.
  - Private VMs allow SSH (22) and HTTP (80) from the Bastion Host.
- SSH Key Pairs (.pem files) for authentication.

4.0: Approach:

4.1: Set up a Bastion Host (Jump Server)

Since the two Linux VMs have private IPs only, we cannot SSH directly into them from a local laptop. Thus, we set up a Bastion Host, which acts as an intermediate jump server.

Steps:

1. Launch a small public EC2 instance (Ubuntu/Amazon Linux).
2. Attach the same VPC and subnet (or ensure it can reach the private VMs).
3. Assign it a public IP.
4. Open port 22 (SSH) in its security group.
5. SSH into the Bastion Host:

```
ssh -i bastion-key.pem ec2-user@<bastion-public-ip>
```

6. From inside the Bastion, SSH into the Private VMs using their private IPs:

```
ssh -i private-key.pem ec2-user@<private-vm-private-ip>
```

- **Reason Why This Step is Needed?**
  - Private VMs have no public exposure for security reasons.
  - The Bastion Host acts as a secure gateway into the private network.
  - Ensures controlled access without exposing internal servers to the internet.

5.0: Implementation:

5.1: On Web Server VM:

- Install Nginx:

```
sudo yum install nginx -y   # Amazon Linux
sudo apt install nginx -y   # Ubuntu
```

- Start and enable Nginx:

```
sudo systemctl start nginx
sudo systemctl enable nginx
```

- Check default page:

```
curl localhost
```

- Create a custom 404 error page:

```
echo "<h1>Custom 404 Error - Page Not Found</h1>" | sudo tee /usr/share/nginx/html/404.html
```

- (Optional) Modify `/etc/nginx/nginx.conf` to configure the custom 404.

5.2 On Client VM:

Create a file you want to transfer:

```
echo "This is a test file from Client VM" > testfile.txt
```

Use SCP to securely transfer the file to Web Server VM:

```
scp -i private-key.pem testfile.txt ec2-user@<web-server-private-ip>:/home/ec2-user/
```

- **Reason Why This Step is Needed?**
  - Demonstrates secure file transfer between private instances inside a VPC.
  - Simulates real-world scenarios like config syncing, data transfer, etc.

6.0: Security Configuration:

- Allow only HTTP (80) and HTTPS (443) traffic in the Web Server security group.
- Allow only SSH (22) traffic from Bastion Host to Client and Web Server VMs.
- Restrict Bastion Host access to your own IP only (inbound rule).

7.0: File Structure:

On Client VM (before transfer):

```
/home/ec2-user/testfile.txt
```

After transfer, on the Web Server VM:

```
/home/ec2-user/testfile.txt
```

8.0: Conclusion:

By setting up a Bastion Host and properly configuring the network and security, it's possible to manage and transfer data between private VMs securely without giving them public IPs. This design ensures a production-like, secured environment for internal communications.