Ansible-Install\_dbserver-PublicIP = "3.81.142.141"

python\_app\_server = "54.145.56.191"

cd .ssh && cat id\_ed25519.pub > authorized\_keys

Certainly! Below is a detailed cloud architecture diagram for ATLAS, incorporating a Host-Based Intrusion Prevention System (HIPS), a Next-Generation Firewall (NGFW), a Web Application Firewall (WAF), and a Security Incident and Event Management tool (SIEM):

```plaintext

+----------------------------------------------+

| Cloud Provider |

| (e.g., AWS, Azure) |

+----------------------------------------------+

|

|

+------------------------------------|-------------------------------------+

| VPC | IAM |

| (Virtual Private Cloud) | (Identity and Access Management) |

| | |

| +-------------------------+ | +-------------------------+ |

| | Private Subnet | | | Public Subnet | |

| | | | | | |

| | +-------------------+ | | | +-------------------+ | |

| | | | | | | | | | |

| | | Database | | | | | Web Application | | |

| | | | | | | | Servers | | |

| | +-------------------+ | | | +-------------------+ | |

| | | HIPS on Laptops | | | | | WAF | | |

| | +-------------------+ | | | +-------------------+ | |

| +-------------------------+ | +-------------------------+ |

| | |

| +-------------------------+ | +-------------------------+ |

| | NGFW for | | | SIEM | |

| | Network Security | | | (Security Incident and | |

| +-------------------------+ | | Event Management) | |

+------------------------------------|-------------------------------------+

|

|

+-----------------|------------------+

| | |

+----------------+ +----------------+ +----------------+

| Laptop | | Laptop | | Laptop |

| with HIPS | | with HIPS | | with HIPS |

+----------------+ +----------------+ +----------------+

```

\*\*Key Components:\*\*

1. \*\*Virtual Private Cloud (VPC):\*\*

- Ensures network isolation and segregation.

2. \*\*IAM (Identity and Access Management):\*\*

- Manages user authentication and authorization.

3. \*\*Private Subnet:\*\*

- Hosts databases and other sensitive resources.

4. \*\*Public Subnet:\*\*

- Hosts public-facing web application servers.

5. \*\*Web Application Servers:\*\*

- Where the web applications are hosted.

6. \*\*WAF (Web Application Firewall):\*\*

- Protects the web application from common web attacks.

7. \*\*HIPS on Laptops:\*\*

- Host-Based Intrusion Prevention System on individual laptops for real-time protection.

8. \*\*NGFW (Next-Generation Firewall):\*\*

- Provides advanced threat protection for network security.

9. \*\*SIEM (Security Incident and Event Management):\*\*

- Centralizes log management and monitors security events.

\*\*Connections:\*\*

- The laptops connect to the cloud through secure channels, ensuring data protection during transit.

- The NGFW monitors and controls traffic to and from the cloud, enhancing network security.

- The WAF protects the web application servers from web-based attacks.

- Logs from various components are aggregated and analyzed by the SIEM for security monitoring.

This architecture aims to create a secure, scalable, and well-organized cloud environment for ATLAS, addressing key security concerns.