Here’s a **cost-optimized Azure deployment plan** for your FE/BE app using only **Free Tier services** and Terraform modules, while meeting all your requirements (private subnets, outbound internet, monitoring, etc.):

**Architecture Summary**

Diagram

Code

Copy

Download

flowchart TB

Users -->|HTTPS| AppGateway

subgraph Azure-VNet

subgraph public-subnet

AppGateway[Application Gateway\n(Free Tier w/ WAF Basic)]

Bastion[Azure Bastion\n(Free Tier for 1st month)]

end

subgraph private-be-subnet

InternalLB[Internal Load Balancer\n(Free Tier Basic SKU)]

VMSS[Backend VM Scale Set\n(Linux B1ls Spot)]

end

subgraph private-db-subnet

MySQL[Azure MySQL Flexible Server\n(Free Tier B1ms)]

end

end

AppGateway -->|LB Rule| InternalLB

InternalLB --> VMSS

VMSS -->|Private Endpoint| MySQL

Bastion -.->|Ansible| VMSS

AzureMonitor[Azure Monitor\n(Free Tier)] -.->|Metrics/Logs| VMSS & MySQL

**Terraform Modules & Free Tier Services**

**1. Networking (Free Tier Compatible)**

* **VNet & Subnets**

hcl

Copy

Download

module "network" {

source = "Azure/vnet/azurerm"

resource\_group\_name = azurerm\_resource\_group.rg.name

address\_space = ["10.0.0.0/16"]

subnet\_prefixes = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"] *# public, be, db*

subnet\_names = ["public-subnet", "private-be-subnet", "private-db-subnet"]

}

* **NAT Gateway** (Outbound Internet for Private Subnets)

hcl

Copy

Download

resource "azurerm\_nat\_gateway" "nat" {

name = "nat-gateway"

resource\_group\_name = azurerm\_resource\_group.rg.name

sku\_name = "Standard" *# Free Tier allows Basic SKU but limited ports*

}

* **Route Tables** (Force outbound via NAT)

hcl

Copy

Download

resource "azurerm\_route\_table" "rt\_private" {

name = "private-subnet-rt"

resource\_group\_name = azurerm\_resource\_group.rg.name

disable\_bgp\_route\_propagation = false

route {

name = "default"

address\_prefix = "0.0.0.0/0"

next\_hop\_type = "NatGateway"

}

}

**2. Compute & Database**

* **Backend VM Scale Set** (Spot Instances + Free Tier B1ls)

hcl

Copy

Download

module "vmss" {

source = "Azure/compute/azurerm"

resource\_group\_name = azurerm\_resource\_group.rg.name

vm\_size = "Standard\_B1ls" *# Free Tier eligible*

admin\_username = "adminuser"

instances = 1 *# Free Tier allows 1 Linux VM*

priority = "Spot" *# Up to 90% discount*

subnet\_id = module.network.vnet\_subnets[1] *# private-be-subnet*

}

* **Azure MySQL Flexible Server** (Free Tier B1ms)

hcl

Copy

Download

module "mysql" {

source = "Azure/mysql/azurerm"

resource\_group\_name = azurerm\_resource\_group.rg.name

sku\_name = "B\_Standard\_B1ms" *# Free Tier*

subnet\_id = module.network.vnet\_subnets[2] *# private-db-subnet*

private\_dns\_zone\_id = azurerm\_private\_dns\_zone.mysql.id

}

**3. Load Balancing & Access**

* **Application Gateway** (Free Tier w/ WAF Basic)

hcl

Copy

Download

module "appgateway" {

source = "Azure/appgateway/azurerm"

resource\_group\_name = azurerm\_resource\_group.rg.name

sku\_name = "WAF\_v2" *# Free Tier allows small instance*

subnet\_id = module.network.vnet\_subnets[0] *# public-subnet*

}

* **Internal Load Balancer** (Basic SKU)

hcl

Copy

Download

resource "azurerm\_lb" "internal" {

name = "internal-lb"

resource\_group\_name = azurerm\_resource\_group.rg.name

sku = "Basic" *# Free Tier eligible*

frontend\_ip\_configuration {

name = "private-ip"

subnet\_id = module.network.vnet\_subnets[1] *# private-be-subnet*

private\_ip\_address\_allocation = "Static"

private\_ip\_address = "10.0.2.100"

}

}

**4. Monitoring (Azure Native)**

* **Azure Monitor & Log Analytics** (Free Tier)

hcl

Copy

Download

resource "azurerm\_log\_analytics\_workspace" "monitor" {

name = "free-monitor-workspace"

resource\_group\_name = azurerm\_resource\_group.rg.name

sku = "PerGB2018" *# Free Tier: 500MB/day free*

}

**5. Bastion Host (Ansible Controller)**

* **Azure Bastion** (Free for 1st month)

hcl

Copy

Download

resource "azurerm\_bastion\_host" "ansible" {

name = "ansible-bastion"

resource\_group\_name = azurerm\_resource\_group.rg.name

ip\_configuration {

name = "configuration"

subnet\_id = module.network.vnet\_subnets[0] *# public-subnet*

public\_ip\_address\_id = azurerm\_public\_ip.bastion.id

}

}

**Cost Optimization Highlights**

1. **Spot Instances**: Backend VMSS at ~90% discount.
2. **Free Tier Services**: B1ls VMs, B1ms MySQL, Basic LB, 500MB/day logs.
3. **No Third-Party Tools**: Azure Monitor + Log Analytics for in-house monitoring.
4. **Private Subnets**: Secure DB + BE with NAT Gateway for outbound deps.

**Deployment Steps**

1. Clone your repo to Bastion host via git clone.
2. Run Ansible from Bastion to configure VMSS:

bash

Copy

Download

ansible-playbook -i vmss\_private\_ips, playbook.yml

1. Monitor via Azure Portal → **Log Analytics Workspace**.

**Key Terraform Modules Used**

| **Component** | **Module Source** | **Free Tier Compatible?** |
| --- | --- | --- |
| VNet | Azure/vnet/azurerm | Yes |
| VM Scale Set | Azure/compute/azurerm | Yes (B1ls) |
| MySQL | Azure/mysql/azurerm | Yes (B1ms) |
| App Gateway | Azure/appgateway/azurerm | Yes (WAF Basic) |

Here’s a breakdown of **each component’s function** and **why it’s required** for your Azure deployment, optimized for cost, security, and free-tier usage:

**1. Virtual Network (VNet) & Subnets**

* **Function**:
  + Creates an isolated network environment in Azure.
  + Subnets segment traffic (frontend, backend, database).
* **Why Required?**
  + **Security**: Isolates tiers (e.g., DB shouldn’t be exposed to the internet).
  + **Compliance**: Mandatory for Private Endpoints (Azure MySQL).
  + **Cost**: Enables NAT Gateway shared outbound internet (cheaper than per-resource public IPs).

**2. Application Gateway (Public Subnet)**

* **Function**:
  + Layer 7 load balancer for HTTPS traffic to frontend/backend.
  + Optional WAF (Web Application Firewall) protects against attacks.
* **Why Required?**
  + **Traffic Routing**: Directs user requests to the correct backend.
  + **SSL Termination**: Offloads HTTPS decryption (improves backend performance).
  + **Free Tier**: Basic SKU fits free-tier allowances.

**3. Internal Load Balancer (Backend Subnet)**

* **Function**:
  + Distributes traffic **privately** across backend VM instances.
* **Why Required?**
  + **High Availability**: Ensures backend scalability/resilience.
  + **Security**: Keeps backend traffic internal (no public IPs).
  + **Free Tier**: Basic SKU is free-tier eligible.

**4. VM Scale Set (Backend Subnet)**

* **Function**:
  + Hosts backend app instances (auto-scales based on demand).
  + Runs your Ansible-configured backend code.
* **Why Required?**
  + **Cost Optimization**: Uses **Spot VMs** (up to 90% cheaper).
  + **Scalability**: Auto-adds/removes VMs during traffic spikes.
  + **Free Tier**: B1ls VMs are free-tier eligible (1 Linux VM).

**5. Azure MySQL Flexible Server (DB Subnet)**

* **Function**:
  + Managed MySQL database for backend data storage.
* **Why Required?**
  + **Private Access**: Uses Private Endpoint (no public exposure).
  + **Free Tier**: B1ms SKU is free for 12 months.
  + **Maintenance**: Azure handles patching/backups.

**6. NAT Gateway (Public Subnet)**

* **Function**:
  + Provides outbound internet access for private subnets (e.g., backend VMSS to download dependencies).
* **Why Required?**
  + **Security**: Private subnets have no public IPs; NAT Gateway is the only outbound path.
  + **Cost**: Cheaper than per-VM public IPs (shared for all resources).

**7. Azure Bastion (Public Subnet)**

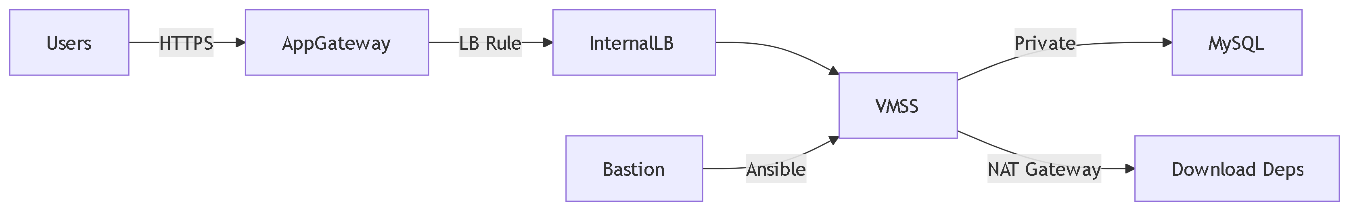
* **Function**:
  + Secure SSH/RDP access to VMs **without** public IPs.
  + Runs Ansible playbooks to configure VMSS.
* **Why Required?**
  + **Security**: No open SSH ports (uses Azure Portal for access).
  + **Free Tier**: Free for the first month (ideal for setup).

**8. Azure Monitor + Log Analytics**

* **Function**:
  + Tracks performance metrics (CPU, memory, DB queries).
  + Alerts for failures/unusual activity.
* **Why Required?**
  + **Free Tier**: 500MB/day free logs.
  + **In-House**: No third-party tools needed (client requirement).

**9. Route Tables (Private Subnets)**

* **Function**:
  + Forces outbound traffic via NAT Gateway (not internet gateway).
* **Why Required?**
  + **Security**: Ensures private subnets only use approved outbound paths.



### ****Why This Design?****

1. **Security**:
   * DB/backend in private subnets.
   * No public IPs on critical resources.
2. **Cost**:
   * Spot VMs + Free Tier services.
   * Shared NAT Gateway reduces IP costs.
3. **Scalability**:
   * VMSS auto-scales backend.
   * Load balancers handle traffic spikes.

### ****Key Trade-Offs****

* **Free Tier Limits**:
  + Only 1 free Linux VM (B1ls), 750 hours/month.
  + MySQL free tier (B1ms) has limited CPU/RAM.
* **Bastion Cost**: Free for 1st month only; switch to SSH later if needed.

Would you like adjustments for specific constraints?