### **Components**

1. **Resource Group**: azurerm\_resource\_group.rg
   * A container that holds related resources for an Azure solution.
2. **Virtual Network (VNet)**: azurerm\_virtual\_network.vnet
   * A virtual network that allows Azure resources to communicate with each other securely.
3. **Subnets**:
   * azurerm\_subnet.external\_lb\_subnet: Subnet for the external load balancer.
   * azurerm\_subnet.firewall\_subnet: Subnet for the firewall.
   * azurerm\_subnet.waf\_subnet: Subnet for the web application firewall.
   * azurerm\_subnet.internal\_lb\_subnet: Subnet for the internal load balancer.
   * azurerm\_subnet.vm\_subnet: Subnet for virtual machines.
   * azurerm\_subnet.bastion\_subnet: Subnet for the bastion host.
4. **Network Security Groups (NSGs)**:
   * azurerm\_network\_security\_group.vm\_nsg: NSG for VMs, allows SSH traffic from the Bastion subnet.
   * azurerm\_network\_security\_group.external\_lb\_nsg: NSG for external load balancer, allows traffic on ports 501 and 502.
5. **Load Balancers**:
   * azurerm\_lb.external\_lb: External load balancer with rules for ports 501 and 502.
   * azurerm\_lb.internal\_lb: Internal load balancer with a rule for port 443.
6. **Public IPs**:
   * azurerm\_public\_ip.external\_lb\_public\_ip: Public IP for the external load balancer.
   * azurerm\_public\_ip.waf\_public\_ip: Public IP for the web application firewall.
   * azurerm\_public\_ip.bastion\_public\_ip: Public IP for the bastion host.
7. **Web Application Firewall (WAF)**:
   * azurerm\_application\_gateway.waf: Application Gateway with a WAF policy.
8. **Virtual Machines (VMs)**:
   * azurerm\_linux\_virtual\_machine.vm1 and azurerm\_linux\_virtual\_machine.vm2: Two Ubuntu VMs.
9. **Bastion Host**:
   * azurerm\_bastion\_host.bastion: Bastion host for secure access to VMs.

### **Example Traffic Flow**

#### **External Traffic to VMs**

1. **User Initiates Traffic**:
   * A user sends a request from the internet to the public IP of the external load balancer (azurerm\_public\_ip.external\_lb\_public\_ip) on port 501.
2. **External Load Balancer**:
   * The external load balancer (azurerm\_lb.external\_lb) receives the request on port 501 and forwards it based on the load balancing rule (azurerm\_lb\_rule.external\_lb\_rule\_501) to one of the backend VMs in the ExternalBackEndAddressPool.
3. **Network Security Group (NSG)**:
   * The azurerm\_network\_security\_group.external\_lb\_nsg attached to the ExternalLBSubnet allows the traffic on port 501.
4. **VM Subnet**:
   * The traffic reaches the VM subnet through the backend pool association and reaches the VM via its network interface (azurerm\_network\_interface.vm\_nic1 or azurerm\_network\_interface.vm\_nic2).

#### **Secure VM Management via Bastion**

1. **User Connects to Bastion Host**:
   * An administrator connects to the Bastion host using its public IP (azurerm\_public\_ip.bastion\_public\_ip).
2. **Bastion Host**:
   * The bastion host (azurerm\_bastion\_host.bastion) provides secure RDP/SSH access to the VMs within the virtual network.
3. **NSG for VM Subnet**:
   * The NSG (azurerm\_network\_security\_group.vm\_nsg) allows SSH traffic from the Bastion subnet (source address prefix 10.0.6.0/24) to the VMs on port 22.
4. **VM Access**:
   * The administrator can securely manage the VMs (azurerm\_linux\_virtual\_machine.vm1 and azurerm\_linux\_virtual\_machine.vm2) using SSH through the Bastion host.

#### **Internal Traffic via Internal Load Balancer**

1. **Internal Service Request**:
   * A service within the virtual network sends a request to the internal load balancer (azurerm\_lb.internal\_lb) on port 443.
2. **Internal Load Balancer**:
   * The internal load balancer forwards the request to one of the VMs in the internal backend pool (azurerm\_lb\_backend\_address\_pool.internal\_backend\_pool) based on the rule (azurerm\_lb\_rule.internal\_lb\_rule\_443).
3. **NSG for VM Subnet**:
   * The NSG associated with the VM subnet (azurerm\_network\_security\_group.vm\_nsg) allows traffic from the internal load balancer.

### **Summary**

* **External Traffic**: User traffic from the internet is balanced by the external load balancer and reaches the VMs through the associated NSG and backend pool.
* **Secure Management**: Administrators use the Bastion host to securely access and manage VMs via SSH.
* **Internal Load Balancing**: Internal services use the internal load balancer to distribute traffic among VMs within the virtual network.

This setup ensures secure and efficient traffic management for both external and internal communication within the Azure infrastructure.

1. Traffic at port 501, as defined in the external\_lb\_rule\_501 resource block, will be allowed through the external load balancer (ELB) to the backend address pool. This traffic is permitted by the associated network security group (NSG) external\_lb\_nsg, which allows inbound traffic on port 501.
2. Traffic at port 502, as defined in the external\_lb\_rule\_502 resource block, will also be allowed through the ELB to the same backend address pool. However, it will also be subject to the Web Application Firewall (WAF) rules configured in the azurerm\_web\_application\_firewall\_policy resource block. This policy defines rules for inspecting and potentially blocking traffic at the application layer based on various conditions, including payload content, headers, etc.

So, in summary:

* Traffic at port 501 goes directly to the backend without inspection by the WAF.
* Traffic at port 502 goes through the WAF, where it may be subject to additional inspection and filtering before reaching the backend.