**Handout: Administering Azure Network Traffic**

This handout provides a comprehensive guide on configuring and managing network traffic within Azure, including routing, load balancing, and monitoring tools.

**1. Overview of Azure Network Traffic Management**

Azure's network traffic management capabilities help maintain reliable, secure, and efficient communication between resources. It supports various routing, balancing, and monitoring features to manage the flow of data in the cloud.

**2. Configuring Network Routing and Endpoints**

**System Routes**:

* **Definition**: Default routes automatically created by Azure to direct traffic between VMs, on-premises networks, and the internet.
* **Key Traffic Flows**:
  + **VMs within the same subnet**
  + **Inter-subnet communication within a VNet**
  + **Internet-bound traffic from VMs**
  + **VNet-to-VNet communication through VPN gateways**

**User-Defined Routes (UDR)**:

* **Purpose**: Customize traffic paths by defining specific routes and next hops, such as a virtual appliance or internet.
* **Example Use Cases**:
  + Directing traffic through Network Virtual Appliances (NVAs)
  + Creating custom routing paths for security or performance reasons

**Service Endpoints**:

* **Usage**: Extend virtual network identity to Azure services over a direct network path.
* **Benefits**: Enhanced security by keeping traffic on the Microsoft network.

**Private Links**:

* **Definition**: Secure private connectivity between Azure resources.
* **Advantages**:
  + Ensures data stays off the public internet.
  + Integrates with peered and on-premises networks for added security.

**3. Configuring Azure Load Balancer**

**Types of Load Balancers**:

* **Public Load Balancer**: Balances incoming traffic from the internet to internal VMs or resources.
* **Internal Load Balancer**: Routes traffic within a virtual network for internal-facing applications.

**Key Features**:

* **Load Balancing Rules**: Define how traffic is distributed across backend pools.
* **Health Probes**: Monitor the health of VMs and adjust the load-balancing strategy accordingly.
* **Session Persistence**: Options include none, client IP, and client IP with protocol to maintain user sessions.

**4. Configuring Azure Application Gateway**

**Overview**:

* **Purpose**: Application-level load balancer for managing HTTP/S traffic.
* **Routing Options**:
  + **Path-based routing**: Directs traffic based on the URL path.
  + **Multi-site routing**: Supports hosting multiple sites behind a single gateway.

**Components**:

* **Frontend IP**: Public or private IP for incoming traffic.
* **Listeners and Routing Rules**: Determine how traffic is handled and directed.
* **Backend Pools**: Groups of web servers to which traffic is routed.
* **Web Application Firewall (WAF)**: Provides protection from common web vulnerabilities.

**5. Configuring Network Watcher**

**Purpose**: A diagnostic and monitoring service for Azure networks.

* **Features**:
  + **IP Flow Verify**: Checks if traffic is allowed to or from a VM.
  + **Next Hop**: Identifies the next routing hop for traffic.
  + **Topology View**: Visualizes network resources and relationships.

**Use Cases**:

* Troubleshooting connectivity issues.
* Visualizing network configurations and flows.

**6. Lab: Implement Traffic Management**

**Scenario**: Set up a hub-and-spoke network topology with Azure Load Balancer and Application Gateway.

**Objectives**:

1. **Provision the Lab Environment**
2. **Configure the Hub and Spoke Topology**
3. **Test VNet Peering**
4. **Set Up Routing**
5. **Deploy Azure Load Balancer**
6. **Configure Application Gateway**

**7. Security Considerations**

**Network Security**:

* **Firewalls and NSGs**: Control inbound and outbound traffic.
* **Private Endpoints**: Enhance data privacy by keeping traffic within a secure network.

**8. Resources and Further Reading**

* **Microsoft Learn Modules**: Interactive learning paths for deeper understanding.
* **Documentation and Tutorials**:
  + Configuring user-defined routes.
  + Setting up load balancing and application gateways.
  + Using Network Watcher for monitoring and diagnostics.

**9. Knowledge Check**

**Sample Questions**:

* What are the differences between public and internal load balancers?
* How do service endpoints enhance network security?
* When should you use a user-defined route?