VPC Routing Patterns

Centralized VPC Routing

Key Concepts:

- Enables connection of multiple Virtual Private Clouds (VPCs)
- Uses Transit Gateway for network interconnectivity
- Supports full resource sharing across connected environments

Deployment Steps:

1. **VPC Attachment**
   - Connect Transit Gateway to VPC via elastic network interfaces
   - Ensure network interface in each Availability Zone
   - Provides cross-VPC communication
2. **Route Table Configuration**
   - Add routes directing traffic to Transit Gateway
   - Use wildcard CIDR blocks (e.g., 10.0.0.0/8)
   - Enables routing across different VPC network ranges

Advanced Routing Techniques:

- Supports routing for hundreds of VPCs
- Allows granular network segmentation
- Provides flexible network design options

Centralized Outbound Routing

Design Principles:

- Dedicated VPC for handling egress internet traffic
- Centralized network security approach
- Cost-efficient NAT gateway management

Implementation Strategy:

- Route internet-bound traffic through specific egress VPC
- Configure route tables to direct traffic to NAT gateway
- Enables comprehensive traffic monitoring and control

VPC Peering

Core Features:

- One-to-one network connection between VPCs
- Enables private IP address communication
- No additional cost for peering connection
- Supports inter-account and inter-region connectivity

Connectivity Limitations:

- **Non-Transitive Peering**
  - Direct connections only between explicitly paired VPCs
  - Prevents unintended network access
  - Enhances network security

Peering Configuration Requirements:

- Non-overlapping CIDR blocks
- Mutual route table configuration
- Potential security group rule updates

Peering Use Cases

Practical Scenarios:

1. **Startup Collaboration**
    - Secure resource sharing
    - Private network infrastructure
    - Faster data exchange
2. **Specific Resource Access**
    - Granular routing to specific subnets
    - Precise IP-level access control
    - Flexible network segmentation

Network Connectivity Options

Site-to-Site VPN:

Connection Establishment Process:

1. Create customer gateway
2. Configure virtual private gateway
3. Set up routing configurations
4. Update security group rules
5. Establish VPN connection
6. Download configuration file

Routing Approaches:

- Dynamic routing (BGP-supported)
- Static routing for non-BGP devices

Direct Connect

Key Characteristics:

- Dedicated private network connection
- Extends on-premises network to AWS
- Consistent network performance
- Increased bandwidth capabilities

Connectivity Methods:

- Private virtual interface
- Public virtual interface
- Transit virtual interface

AWS PrivateLink

Connectivity Advantages:

- Private application-level connections
- Supports overlapping IP address ranges
- Unidirectional connection initiation
- Secure inter-VPC communication

Advanced Networking Strategies

High Availability Configurations

Recommended Practices:

- Multiple Direct Connect locations
- Redundant hardware deployment
- Active/active connection strategies
- Fault-tolerant network design

Transit Gateway Peering

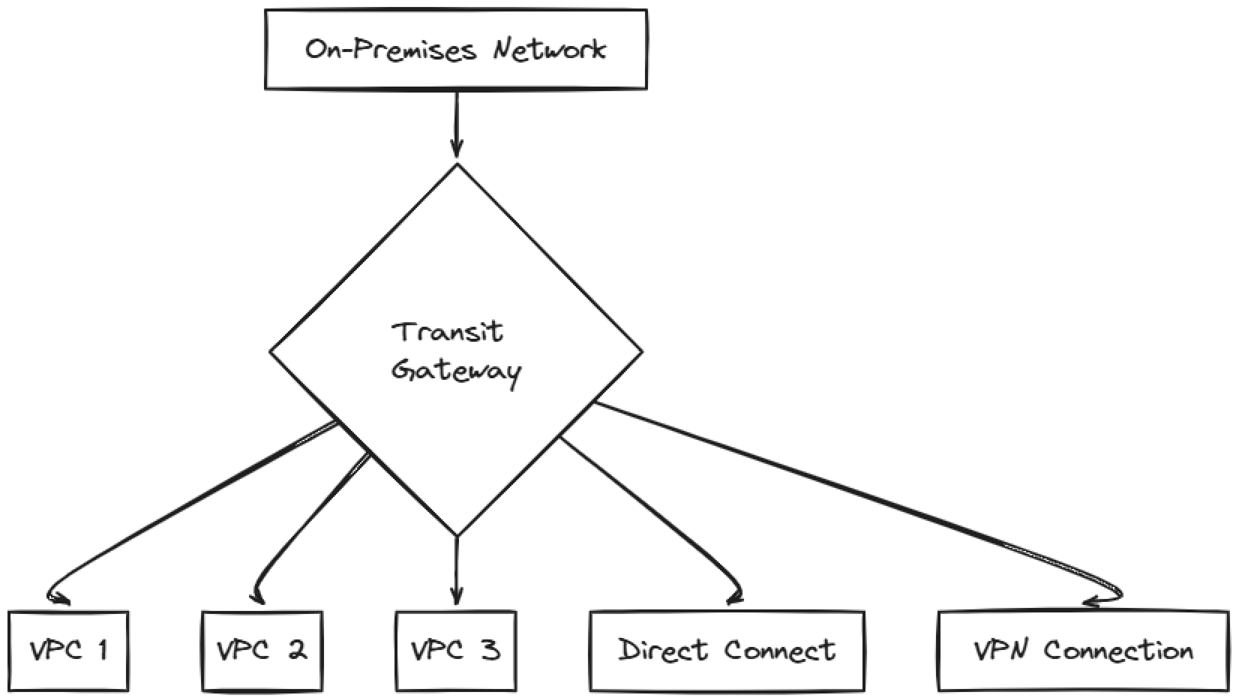
Cross-Region/Cross-Account Connectivity:

- Enables network traffic between different AWS environments
- Supports inter-region and inter-account communication
- Secure traffic routing without public internet traversal

Recommended Network Design Principles

1. Minimize network complexity
2. Implement granular access controls
3. Design for scalability
4. Prioritize security
5. Ensure high availability
6. Optimize cost-efficiency

Mermaid Diagram: Network Connectivity Flow



Key Takeaways

- Understand diverse AWS networking options
- Implement secure, scalable network architectures
- Leverage Transit Gateway for complex network designs
- Prioritize network segmentation and access control