Assignment 4 Submission

Submission ID: 673f49b8f6c8cf56feced71c

Submitted On: 2024-11-21 10:54:48

Net ID: jy451478

Answer 1:

Correct Use Case:

1. NAT Gateways enable private subnets to securely access the internet for updates or API calls [1] .
2. They provide secure outbound connectivity without exposing private resources.

Issues with Deploying NAT Gateways in Every Subnet:

1. Complexity : Not all private subnets (e.g., database instances) require internet access, making this unnecessary.
2. Cost : Deploying NAT Gateways in every subnet leads to excessive uptime and data processing charges.

Improved Approach:

1. Deploy one NAT Gateway per Availability Zone and route all private subnets in that AZ to it.

2. This reduces costs, simplifies architecture, and maintains high availability.

Answer 2:

* A fully meshed VPC peering setup enables communication between all VPCs but becomes complex and inefficient as the architecture scales.

Issues with Fully Meshed VPC Peering:

1. Complexity : Fully meshed peering becomes unmanageable as the number of VPCs grows, leading to operational overhead.
2. Routing Challenges : Managing numerous CIDR blocks and routes increases the risk of errors, such as overlaps or missing routes.

Improved Approach:

1. Use AWS Transit Gateway[2] : A Transit Gateway simplifies network architecture as a centralized hub for connecting multiple VPCs and hybrid connections (VPN, Direct Connect).
2. Scalability and Efficiency : Transit Gateway supports thousands of VPCs, reduces routing complexity, and eliminates the need for complex peering relationships across regions.

Answer 3:

* IPsec tunnels provide strong encryption for in-transit traffic but are often unnecessary for VPC internal communication [3] .

Issues with Using IPsec Tunnels:

1. Performance Impact : IPsec encryption introduces latency and can degrade network performance.
2. Increased Overhead : Setting up and managing IPsec tunnels between VPCs is complex and requires additional configuration.

Improved Approach:

1. Use TLS/SSL[4] : Leverage AWS?s built-in TLS/SSL encryption for securing in-transit data between instances, services, and across VPCs.
2. Use AWS PrivateLink[5] : Establish secure connections between VPCs without exposing data to the public internet, enhancing both security and simplicity.

Answer 4:

* Applying the same NACLs to all subnets simplifies configuration but fails to address subnet-specific security requirements [6] .

Issues with Using the Same NACLs for All Subnets:

1. Lack of Security : Different subnets require different traffic rules; using the same NACL increases exposure to threats.

2. Violates Least Privilege : Generic permissions grant unnecessary access, undermining the principle of least privilege.

Improved Approach:

1. Subnet-Specific NACLs : Assign tailored NACLs based on the subnet type (e.g., stricter rules for private subnets, and open rules for public subnets).

2. Use Security Groups : Add instance-level traffic control with Security Groups to enhance security, aligning with AWS best practices [7] .

Answer 5:

* Public APIs provide convenient access but expose sensitive data to potential threats and performance issues.

Issues with Using Public APIs for User Profiles:

1. Security Risks : Public APIs increase exposure to threats as they can be accessed by anyone.

2. High Latency : Public APIs rely on the internet, leading to higher latency compared to private connections.

Improved Approach:

1. Use API Gateway with VPC : Create and manage API endpoints using API Gateway[8] integrated with the VPC, ensuring secure access without exposing APIs to the public.

2. Leverage AWS PrivateLink : Use PrivateLink to keep API traffic within the VPC, ensuring data never leaves the AWS network, and enhancing security and performance.

Answer 6:

* Transit Gateway provides centralized traffic routing for VPCs and hybrid connections, simplifying network management.

Issues with Mixing VPC Peering and Direct Connect/VPN:

1. Incorrect Assumption : AWS Transit Gateway can connect to on-premises networks using Direct Connect Gateway or Site-to-Site VPN.

2. Increased Complexity : Using a mix of VPC peering and Direct Connect/VPN creates fragmented routing and adds unnecessary operational overhead.

Improved Approach:

1. Use Transit Gateway for Centralized Routing : AWS Transit Gateway provides a scalable and simplified solution to route traffic centrally between VPCs and on-premises networks.

2. Hybrid Connectivity : Connect the on-premises network to Transit Gateway via Direct Connect Gateway or Site-to-Site VPN for seamless integration.

References

[1] ?NAT Gateway Scenarios,? docs.aws.amazon.com [online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-scenarios.html . [Accessed: Nov 21st, 2024].

[2] ?AWS Transit Gateway,? aws.amazon.com [online]. Available: https://aws.amazon.com/transit-gateway/ . [Accessed: Nov 21st , 2024].

[3] ?What is IPsec?,? nordlayer.com [online]. Available: https://nordlayer.com/learn/vpn/ipsec/ . [Accessed: Nov 21st , 2024].

[4] ?What is an SSL Certificate?,? aws.amazon.com [online]. Available: https://aws.amazon.com/what-is/ssl-certificate/ . [Accessed: Nov 21st , 2024].

[5] ?AWS PrivateLink,? aws.amazon.com [online]. Available: https://aws.amazon.com/privatelink/ . [Accessed: Nov 21st , 2024].

[6] ?Network ACLs,? docs.aws.amazon.com [online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html . [Accessed: Nov 21st , 2024].

[7] ?Security Groups and Network ACLs,? docs.aws.amazon.com [online]. Available: https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/security-groups-and-network-acls-bp5.html . [Accessed: Nov 21st , 2024].

[8] ?Amazon API Gateway,? aws.amazon.com [online]. Available: https://aws.amazon.com/api-gateway/ . [Accessed: Nov 21st , 2024].