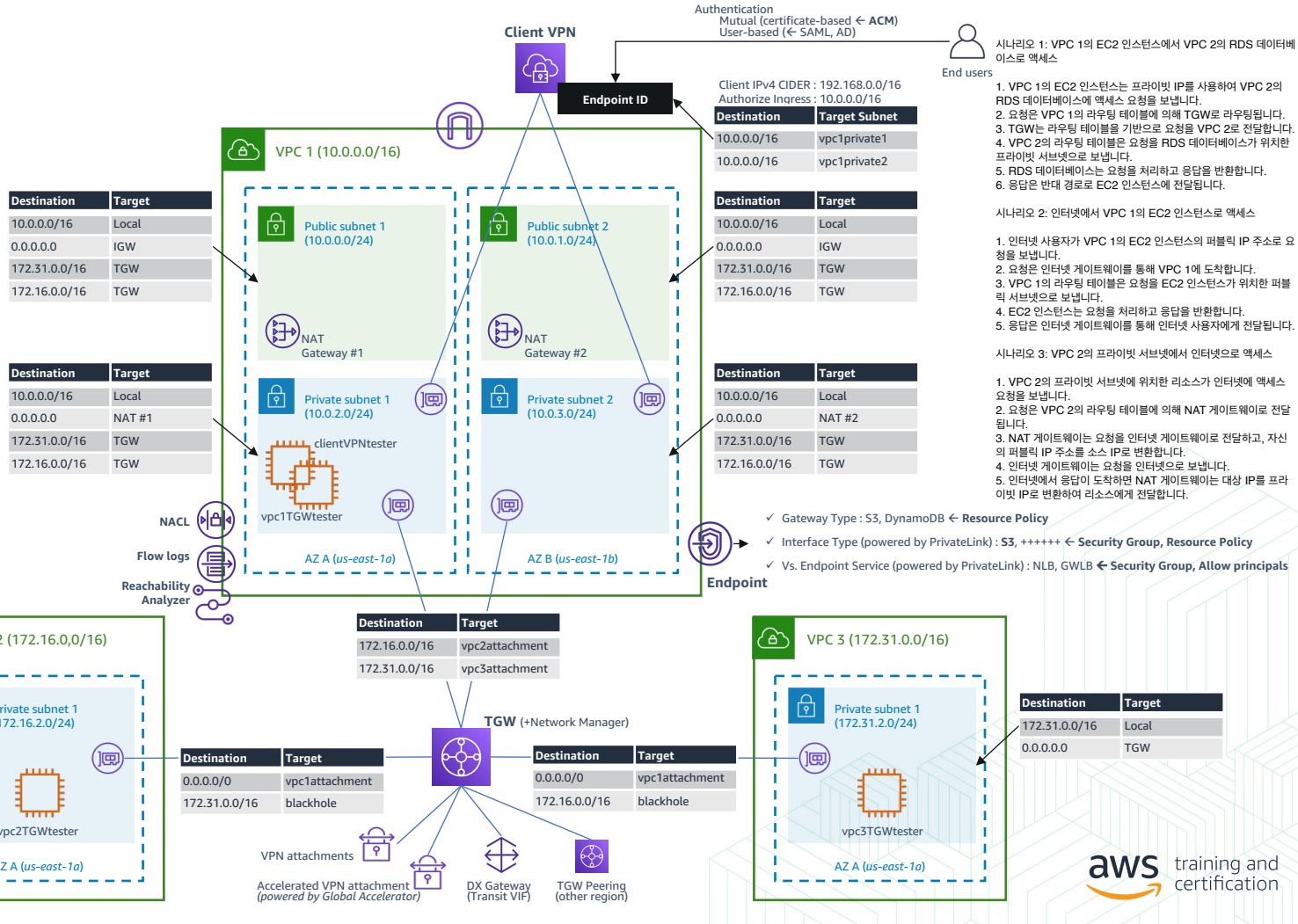
AWS VPC – TGW, ClientVPN

중앙에 있는 TGW는 VPC 간의 트래픽을 라우팅하는 핵심 구성 요소입니다. 왼쪽과 오른쪽에는 각각 VPC가 있습니다. 각 VPC에는 퍼블릭 서브넷과 프라이빗 서브넷이 포함되어 있으며, 퍼블릭 서브넷에는 EC2 인스턴스가, 프라이빗 서브넷에는 RDS 데이터베이스가 배치되어 있습니다.

각 VPC는 인터넷 게이트웨이를 통해 인터넷에 연결되어 있으며, NAT 게이트웨이를 사용하여 프라이빗 서브넷의 리소스가 인터넷에 액세스할 수 있도록 합니다.

VPC 간의 통신은 TGW를 통해 이루어집니다. 각 VPC는 VPC 연결을 통해 TGW에 연결되며, TGW 라우팅 테이블은 VPC 간의 트래픽 흐름을 제어합니다.



시나리오 1: VPC 1의 EC2 인스턴스에서 VPC 2의 RDS 데이터베이스로 액세스

1. VPC 1의 EC2 인스턴스는 프라이빗 IP를 사용하여 VPC 2의 RDS 데이터베이스에 액세스 요청을 보냅니다.
2. 요청은 VPC 1의 라우팅 테이블에 의해 TGW로 라우팅됩니다.
3. TGW는 라우팅 테이블을 기반으로 요청을 VPC 2로 전달합니다.
4. VPC 2의 라우팅 테이블은 요청을 RDS 데이터베이스가 위치한 프라이빗 서브넷으로 보냅니다.
5. RDS 데이터베이스는 요청을 처리하고 응답을 반환합니다.
6. 응답은 반대 경로로 EC2 인스턴스에 전달됩니다.

시나리오 2: 인터넷에서 VPC 1의 EC2 인스턴스로 액세스

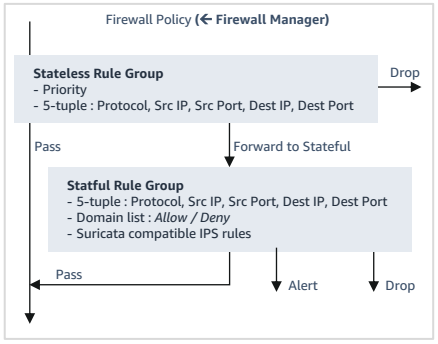
1. 인터넷 사용자가 VPC 1의 EC2 인스턴스의 퍼블릭 IP 주소로 요청을 보냅니다.
2. 요청은 인터넷 게이트웨이를 통해 VPC 1에 도착합니다.
3. VPC 1의 라우팅 테이블은 요청을 EC2 인스턴스가 위치한 퍼블릭 서브넷으로 보냅니다.
4. EC2 인스턴스는 요청을 처리하고 응답을 반환합니다.
5. 응답은 인터넷 게이트웨이를 통해 인터넷 사용자에게 전달됩니다.

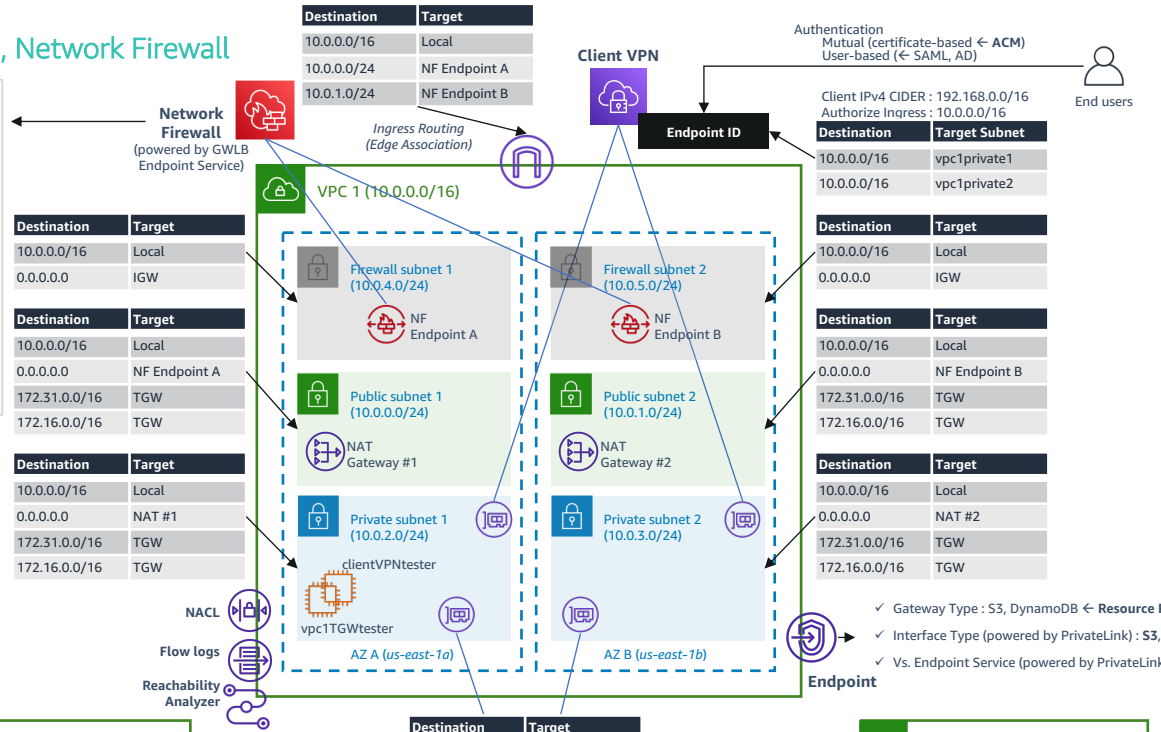
시나리오 3: VPC 2의 프라이빗 서브넷에서 인터넷으로 액세스

1. VPC 2의 프라이빗 서브넷에 위치한 리소스가 인터넷에 액세스 요청을 보냅니다.
2. 요청은 VPC 2의 라우팅 테이블에 의해 NAT 게이트웨이로 전달됩니다.
3. NAT 게이트웨이는 요청을 인터넷 게이트웨이로 전달하고, 자신의 퍼블릭 IP 주소를 소스 IP로 변환합니다.
4. 인터넷 게이트웨이는 요청을 인터넷으로 보냅니다.
5. 인터넷에서 응답이 도착하면 NAT 게이트웨이는 대상 IP를 프라이빗 IP로 변환하여 리소스에게 전달합니다.

aws training and certification

AWS VPC – TGW, ClientVPN, Network Firewall





aws training and certification