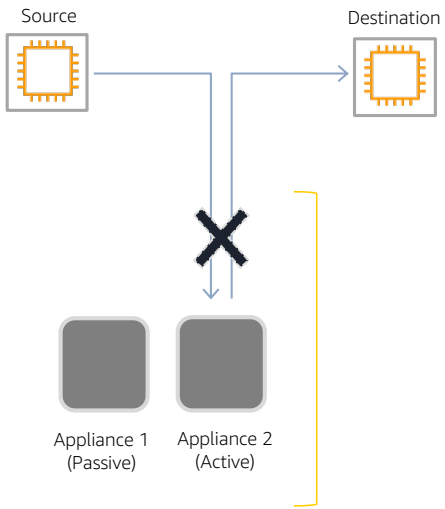
aws Professional Services

GWLB(GateWay Load Balancer)

박병화 (bhpark@amazon.com)
Sr. Security Consultant
AWS Proserve

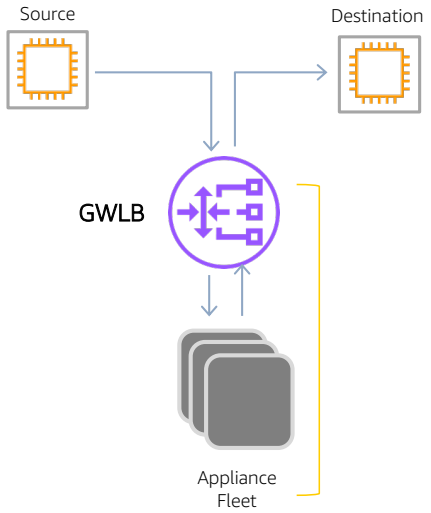
GWLB (Gateway Load Balancer)

- GWLB는 다수의 가상 보안전용솔루션에 대한 로드 밸런싱 및 확장 기능을 제공하고, 선호하는 보안 솔루션 구축의 용이성, 고가용성, 복원성을 제공
- 가상 보안전용솔루션 Pool(Fleet)로 라우팅 하기 위한 게이트웨이를 제공하여, 심플하고 효율적인 네트워크 아키텍처 구현하며, 운영 오버헤드와 비용 감소
- AWS Marketplace에서 주요 보안솔루션을 쉽게 배포할 수 있으며 처리 용량에 따라 자동으로 확장되며, 헬스체크를 통해 정상 동작하는 보안 솔루션으로만 트래픽을 라우팅함으로써 애플리케이션 및 워크로드의 가용성 향상
- Client IP 유지가 가능한 간결한 설계로 트래픽 가시성의 확보와 보안솔루션 구축/연동 시 아키텍처 설계의 단순화
- 워크로드에 따른 서비스 체이닝을 구현함으로써, 워크로드 별로 원하는 보안 솔루션을 묶어 연동



GWLB 사용 전

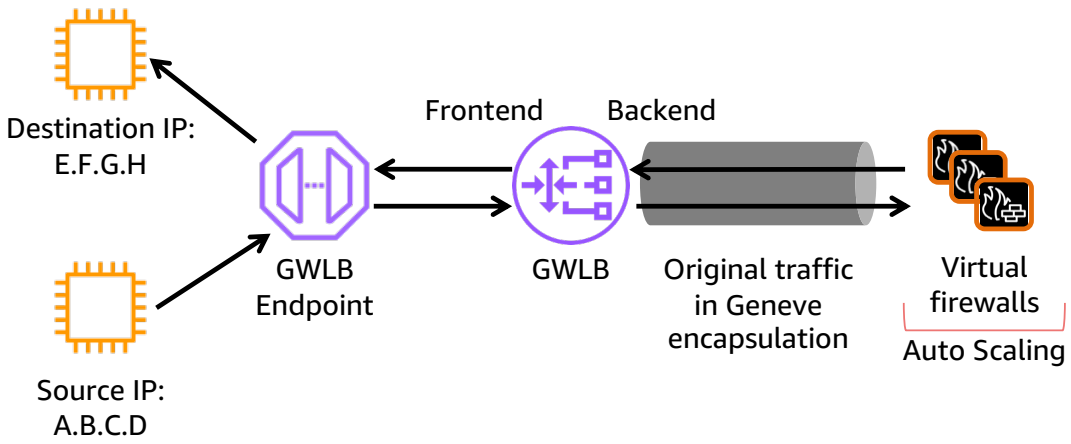
- 장애의 중심점
- 제한된 규모
- 패시브 VM의 유휴 상태
- 혼합 관리 도메인



GWLB 사용 후

- 고가용성
- 수평적 확장
- 부하 분산
- Transparent 구성

GWLB 장점



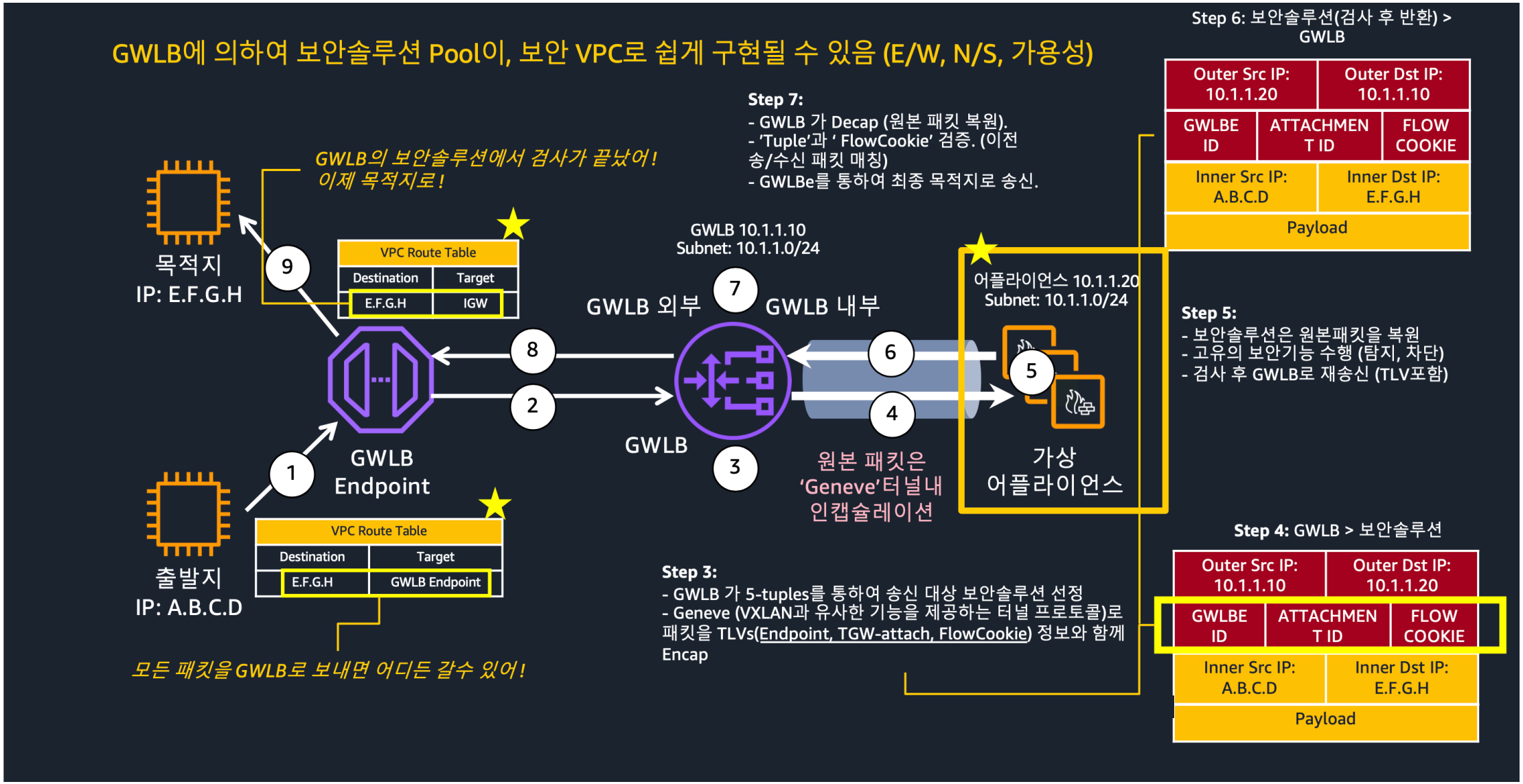
GWLB :

- Elastic Load Balancing 제품군의 로드 밸런서 유형
- 타사 가상 어플라이언스를 쉽게 배포, 확장 및 관리 용이
- GWLB 엔드포인트를 통해 게이트웨이 로드 밸런서로 라우팅되는 트래픽
- 투명한 네트워크 게이트웨이와 로드 밸런서의 조합

GWLB 장점 :

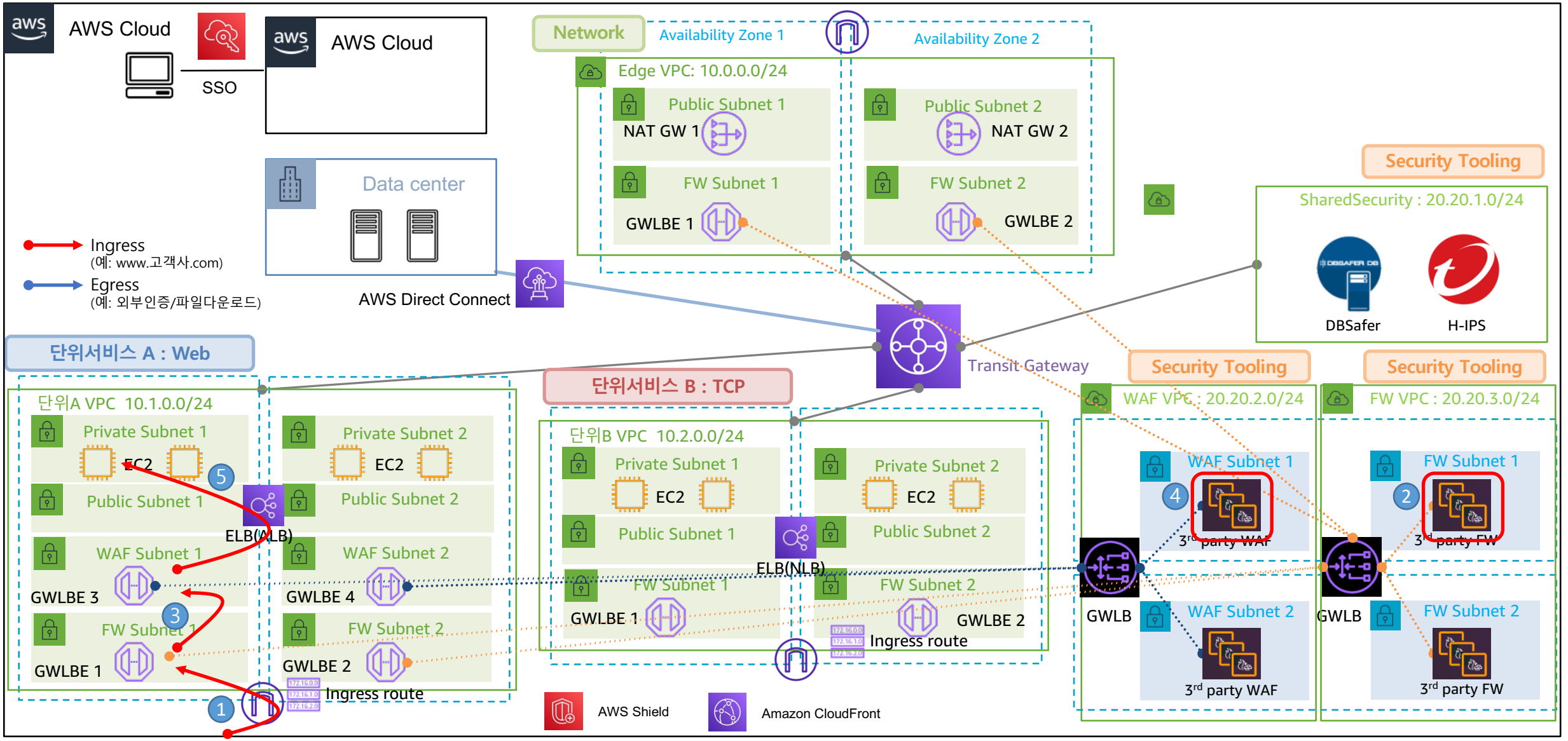
- 네트워크 트래픽에 투명, 소스 트래픽 변경 없음
- 어플라이언스에 수평 확장 제공
- 어플라이언스에 내결함성(fault tolerance) 제공
- 보안 및 사용자 관리 도메인을 분리하며, 서로 다른 VPC 및 AWS 계정에서 공유
- 어플라이언스를 서비스로 제공(예: Firewall as a Service)

3rd Party 연동 아키텍처 (Geneve Protocol) 및 통신방식



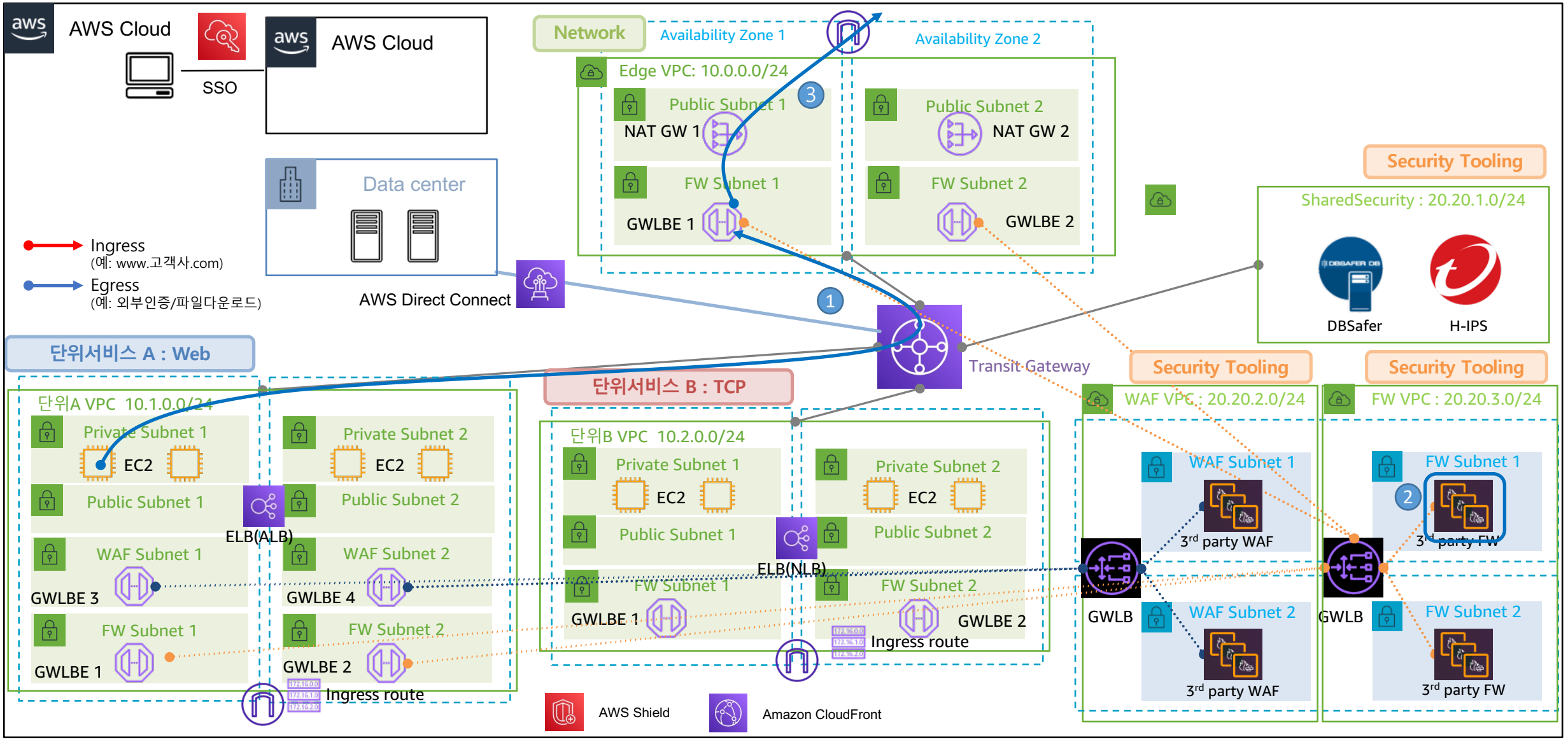
3rd Party 연동 트래픽 플로우 (분산형 Ingress)

AWS 클라우드 환경에서 기능이 검증되고 고객사가 현재 운영 중에 있는 3rd Party 벤더의 웹방화벽과 네트워크 방화벽으로 구성하는 아키텍처



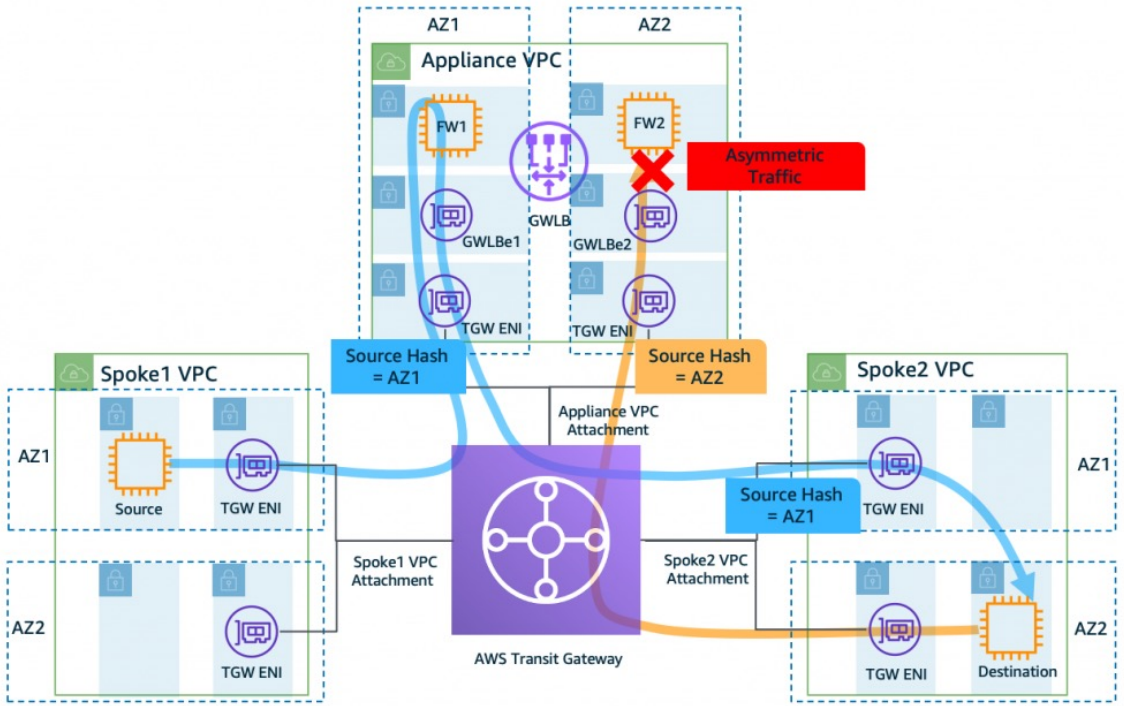
3rd Party 연동 트래픽 플로우 (집중형 Egress)

AWS 클라우드 환경에서 기능이 검증되고 고객사가 현재 운영 중에 있는 3rd Party 벤더의 웹방화벽과 네트워크 방화벽으로 구성하는 아키텍처

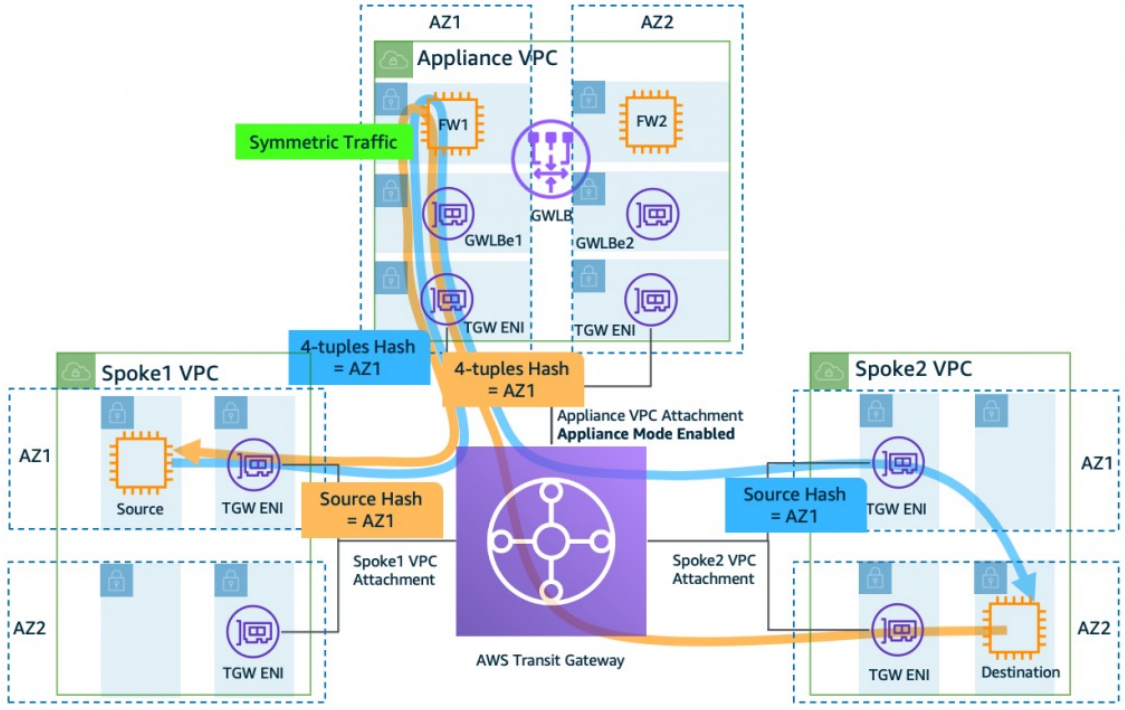


다중 AZ환경에서 대칭형(Symmetric) 플로우를 위한 TGW 어플라이언스 모드 설정

- TGW Appliance Mode가 활성화 되어 있지 않는 경우, VPC B의 AZ2에서 시작된 응답 트래픽은 Transit Gateway에 의해 VPC C의 동일한 AZ 2로 라우팅. 따라서 AZ2의 어플라이언스가 VPC A에 있는 소스의 원래 요청을 인식하지 못하기 때문에 트래픽 드랍
- 다중 AZ 환경에서 보안 장비로의 트래픽 대칭형 플로우를 만들기 위해 Transit gateway 어플라이언스 모드 활성화 필요

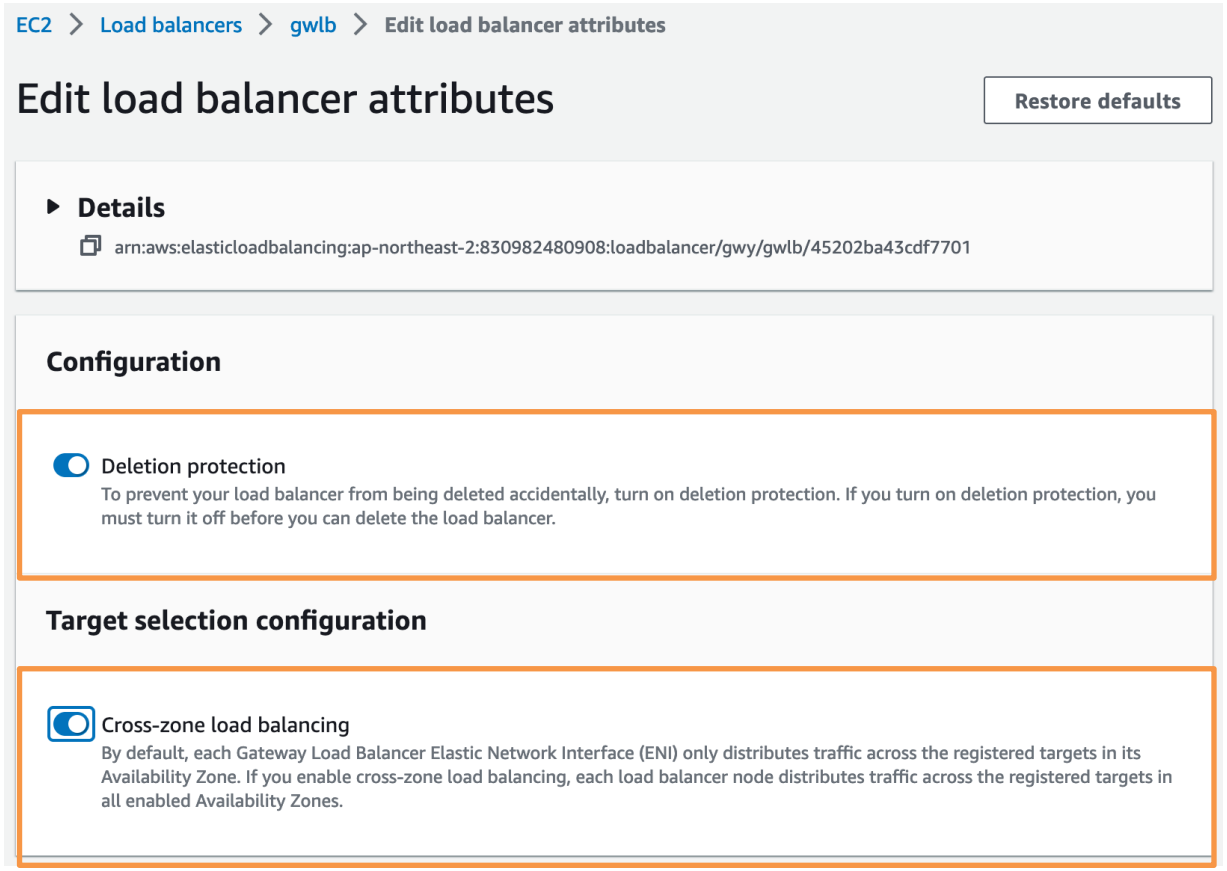


- 비대칭형 플로우 발생 : TGW 어플라이언스 모드 비활성화(기본값)



- 대칭형 플로우 발생 : TGW 어플라이언스 모드 활성화

GWLB 부하분산 상세 설정



<권고 설정>

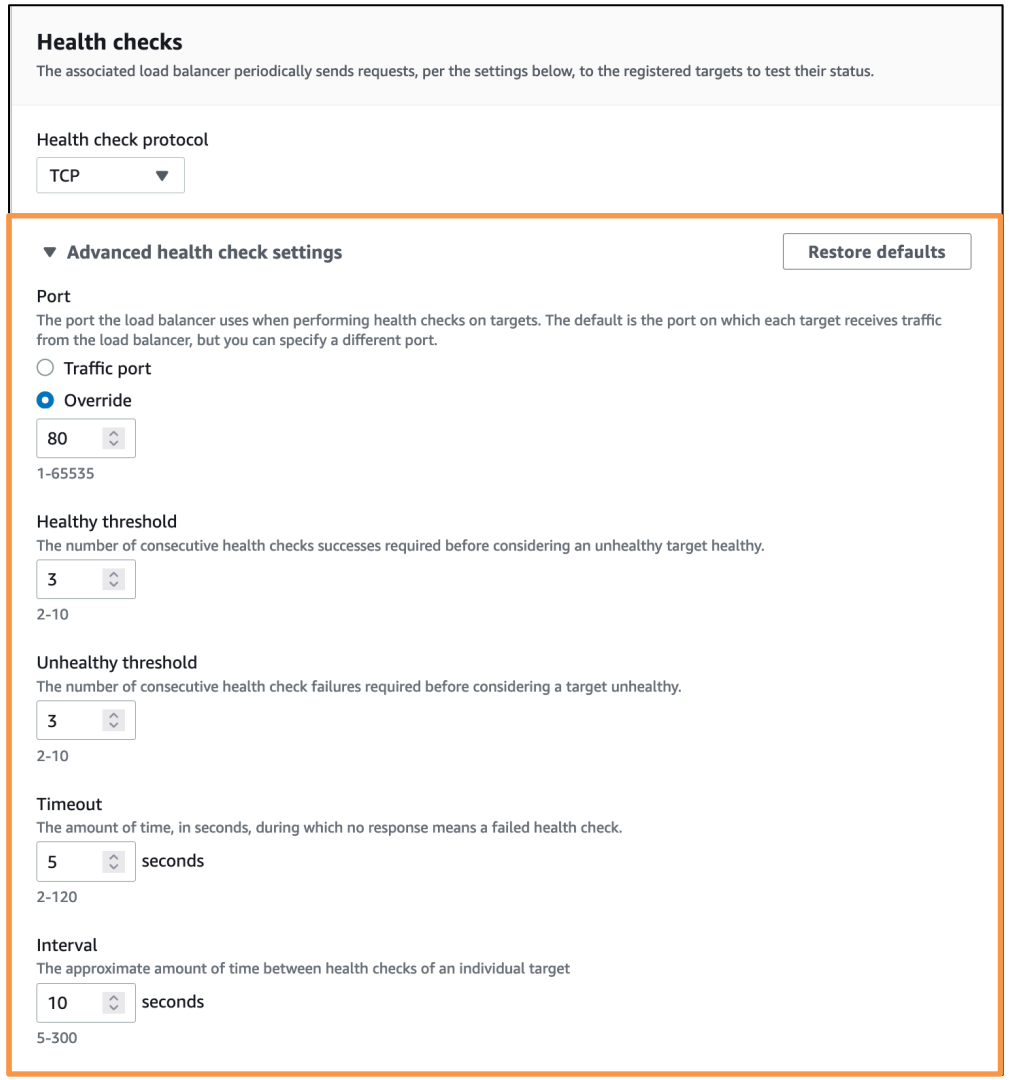
Deletion Protection :

- GWLB 삭제 사고를 방지하기 위해 삭제보호(Deletion Protection) 기능을 켜는 것을 권고 (default : 비활성화)
- GWLB 삭제가 필요한 경우, 해당 기능을 수동으로 비활성화 시킨 후 삭제해야 삭제 실행됨

Cross-zone Load balancing :

- 기본적으로 각 GWLB Elastic Network Interface (ENI)는 해당 가용 영역에 등록된 타겟 대상에만 트래픽 분산 수행
- Cross-zone Load Balacing을 활성화하면, 모든 가용 영역에서 등록된 타겟 대상으로 트래픽을 분산 수행
- 3rd Party 보안솔루션의 경우, 2개의 AZ에 각각 1기씩(총 2기) VM을 구성할 예정이므로, Cross-zone Load balancing 활성화 권고

GWLB 타겟 그룹 상세 설정



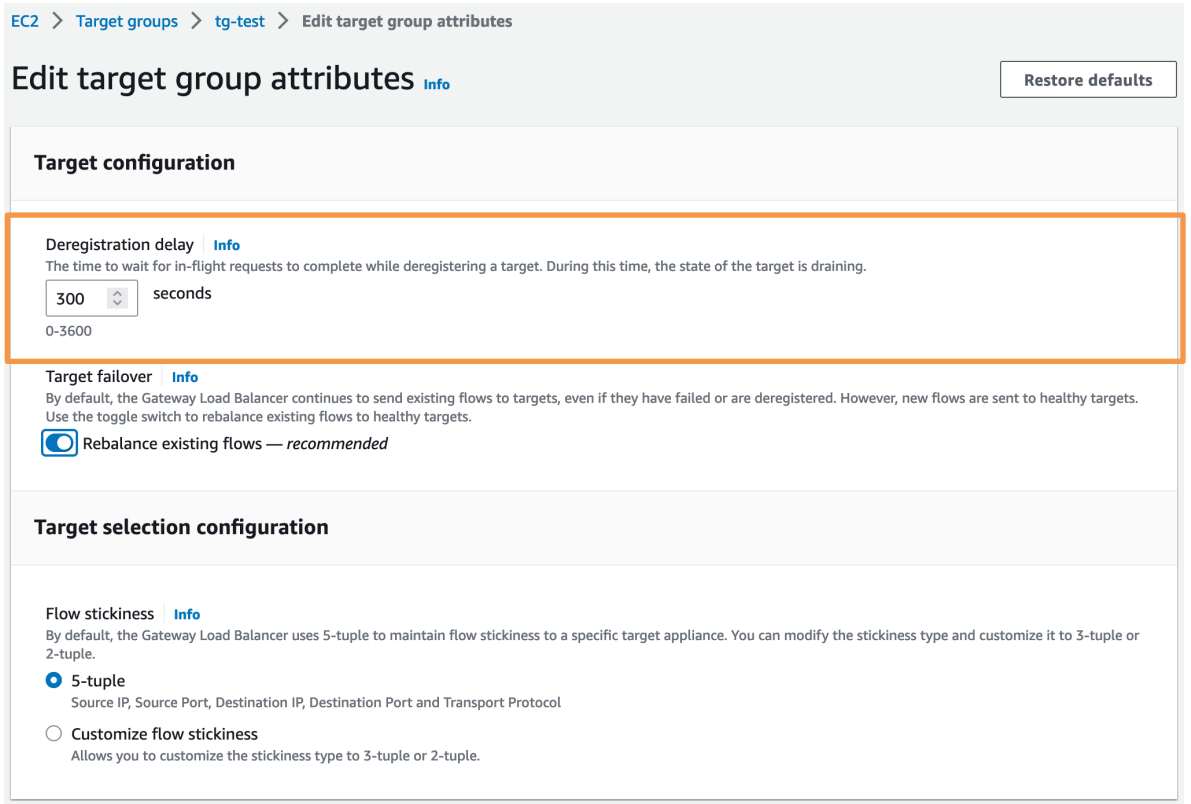
<권고 설정(기본값)>

Health checks :

- Health check protocol : TCP, HTTP, HTTPS 선택
- Geneve (UDP :6081)를 통해 보안 솔루션VM과 인캡슐레이션 통신을 하며, 보안 솔루션 VM의 가용성 체크를 위한 헬스체크
- 포트 (1-65535) : 로드 밸런서가 대상에서 상태 확인을 수행할 때 사용하는 포트로 기본값은 각 대상이 로드 밸런서에서 트래픽을 수신하는 포트이며, 다른 포트 지정 가능
- Healthy 임계값 (2-10) : Unhealthy 대상을 Healthy로 간주하기 전에 필요한 연속 상태 확인 성공 횟수
- Unhealthy 임계값 (2-10) : 대상을 Unhealthy로 간주하기 전에 필요한 연속 상태 확인 실패 횟수
- Timeout (2-120) : 상태 확인 실패로 판단하는 응답 없는 시간
- Interval (5-300) : Health check 간격

모든 값을 최소로 변경 시, 보안 VM 상태(healthy/unhealthy)에 플래핑을 유발할 수 있으므로, 값 변경에 주의 필요

GWLB 타겟 그룹 상세 설정

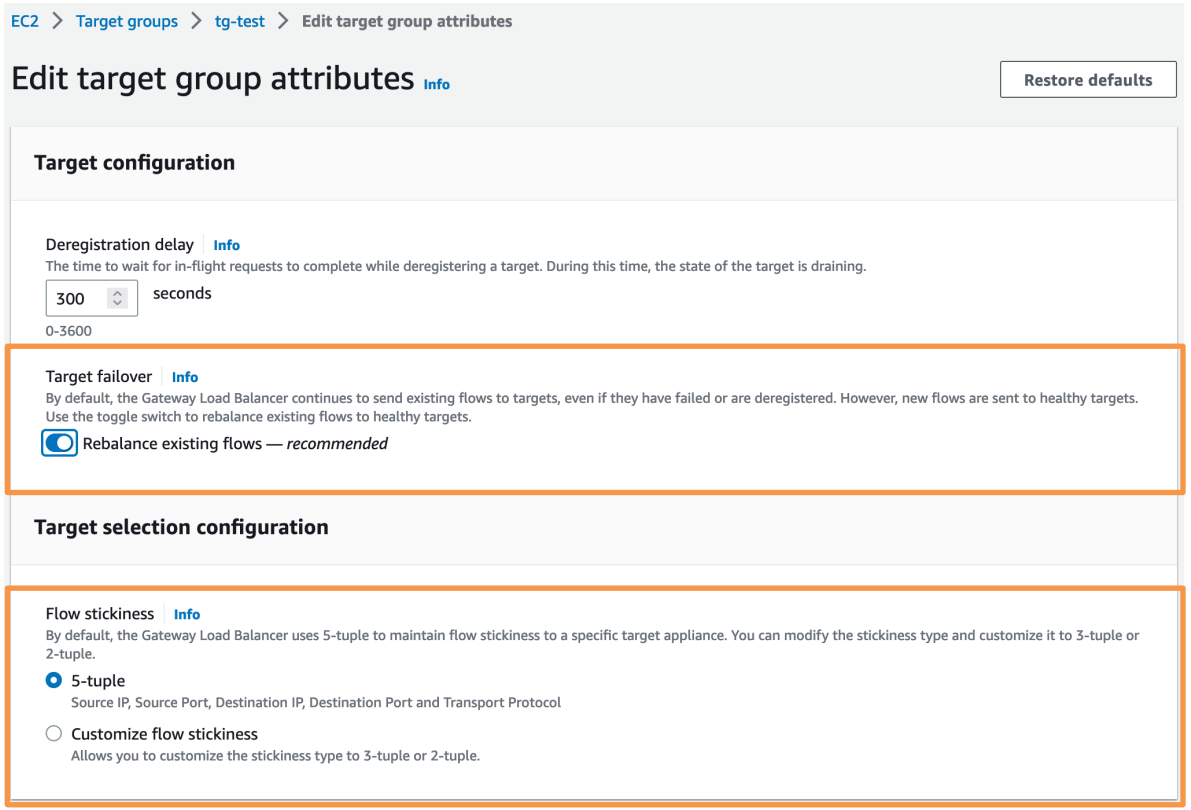


<권고 설정>

Deregistration delay(GWLB의 타겟 등록 취소 지연) :

- 타겟 등록을 취소하는 동안 진행 중인 요청이 완료될 때까지 기다리는 시간으로, 해당 시간 동안 타겟의 상태는 고갈(draining) 상태 유지
- 신규 플로우(New flows) : 타겟 등록이 취소된 대상에 대한 신규 플로우 전송 중지
- 기존 흐름(Existing flows) : GWLB는 프로토콜을 기반으로 기존 흐름 처리 (TCP 프로토콜에 대한 기존 흐름은 350초 이상 유휴 상태인 경우 닫히고, TCP가 아닌 모든 프로토콜에 대한 기존 흐름은 120초 이상 유휴 상태인 경우 닫힘)
- 타겟등록 취소 지연 제한 시간이 만료되면 대상이 사용되지 않는(unused) 상태로 전환
- **3rd Party 의 경우, GWLB의 각 프로토콜 Timeout 시간보다 적게 설정 필수 (예, TCP : 300초, UDP : 60초)**

GWLB 타겟 그룹 상세 설정



<권고 설정>

Target failover :

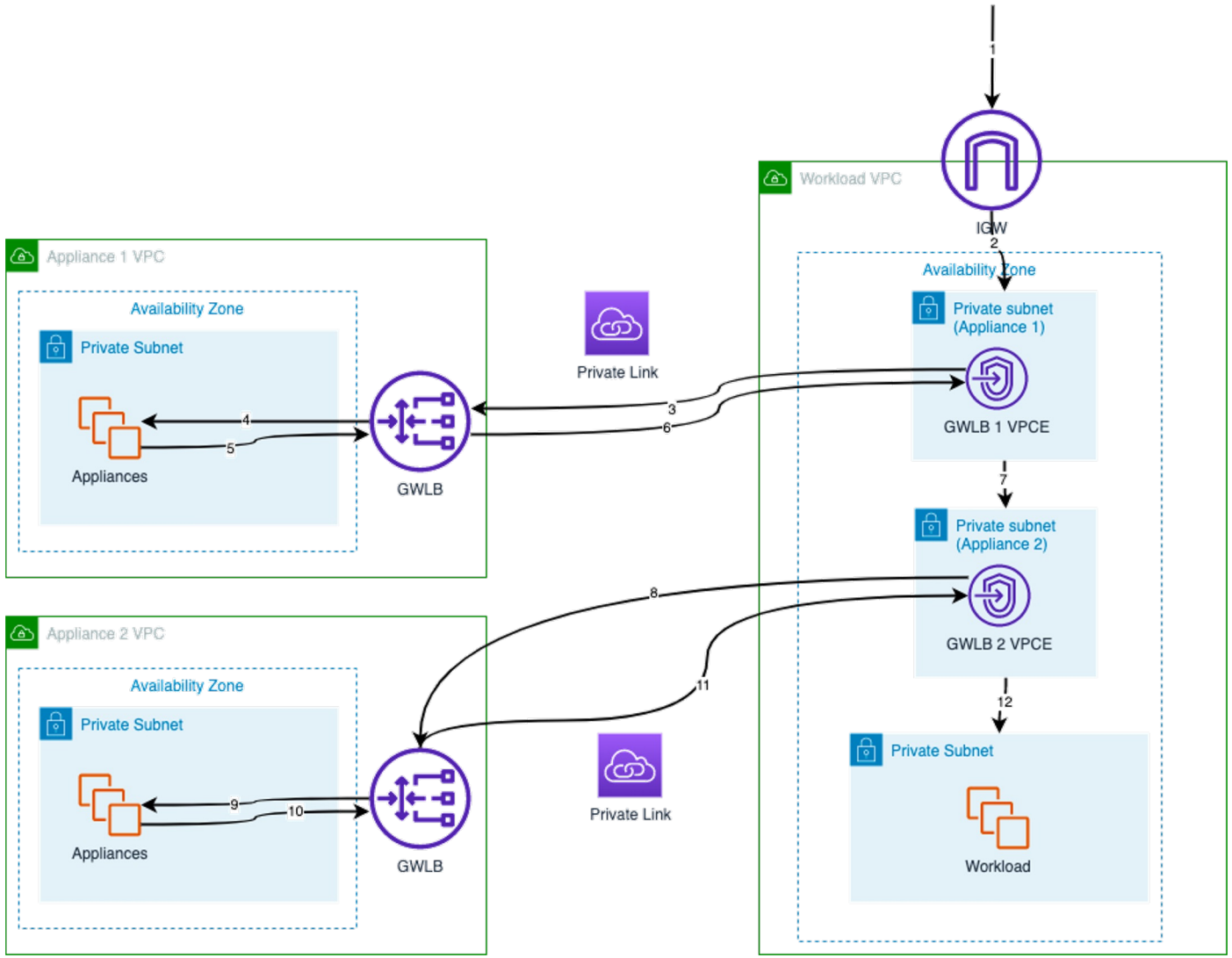
- 기본적으로 GWLB는 타겟 대상이 실패했거나 등록 취소되더라도, 기존 플로우에 대해 계속해서 전송하며, 신규 플로우는 정상 타겟 대상으로 전송
- Rebalance existing flows : 기능을 사용하면, 기존 플로우도 신규 플로우 같이 정상 타겟 대상으로만 전송하도록 재조정

Flow stickiness :

- GWLB는 5-Tuple(기본값)을 사용하여 특정 대상 보안솔루션에 대한 흐름 고정성 유지하며, Customize flow stickiness 수정하여 3-Tuple 또는 2-Tuple 선택 가능
- 값을 수정하기 전에 열려 있는 모든 세션을 종료하는 것을 권고

GWLB 서비스 체이닝 설계

- 2개 이상의 보안 장비군으로 서비스 체이닝을 구성할 경우, GWLB-E 티어별로 라우팅 홉을 적용함으로써, 보안 서비스 체이닝을 지원



GWLB : 3rd Party 및 AZ 장애 failover 설계

- 3rd Party 보안 서비스의 가용성은 3rd Party 장애 또는 AZ 장애라는 두 가지를 고려해서 설계해야 합니다. 다른 로드밸런서(ALB/NLB)와 마찬가지로 GWLB는 VPC에서 실행되고 AZ 장애에 대한 복원력이 있는 리전 서비스입니다. 그러나 GWLB 엔드포인트는 AZ 리소스이므로 고객은 두개 이상의 AZ에 GWLB 엔드포인트를 각각 생성해야 합니다. 그리고 GWLB는 다른 로드 밸런서와 달리 아래와 같은 장애 시나리오가 발생할 때, 플로우 관리 측면에서 다르게 동작합니다.

장애 시나리오	Cross-zone Load balancing	기존 플로우	신규 플로우
AZ 1에 특정 FW 장애 경우	비활성화	타임아웃 또는 클라이언트로부터 Reset 필요	같은 AZ안의 Healthy FW로 전달
AZ 1에 특정 FW 장애 경우	활성화	타임아웃 또는 클라이언트로부터 Reset 필요	같은 AZ 또는 다른 AZ의 Healthy FW로 전달
AZ 1에 모든 FW 장애 경우	비활성화	타임아웃 또는 최소한 하나의 FW 복구전까지 드랍	타임아웃 또는 최소한 하나의 FW 복구전까지 드랍
AZ 1에 모든 FW 장애 경우	활성화	타임아웃 또는 클라이언트로부터 Reset 필요	다른 AZ의 Healthy FW로 전달
NFW/WAF 별로 2개의 AZ에 각각 1기씩의 총 2기의 VM 구성 시, 발생할 수 있는 시나리오			
AWS Region의 특정 AZ 1장애	비활성화 또는 활성화	다른 AZ로 전달되므로 영향 없음	다른 AZ로 전달되므로 영향 없음

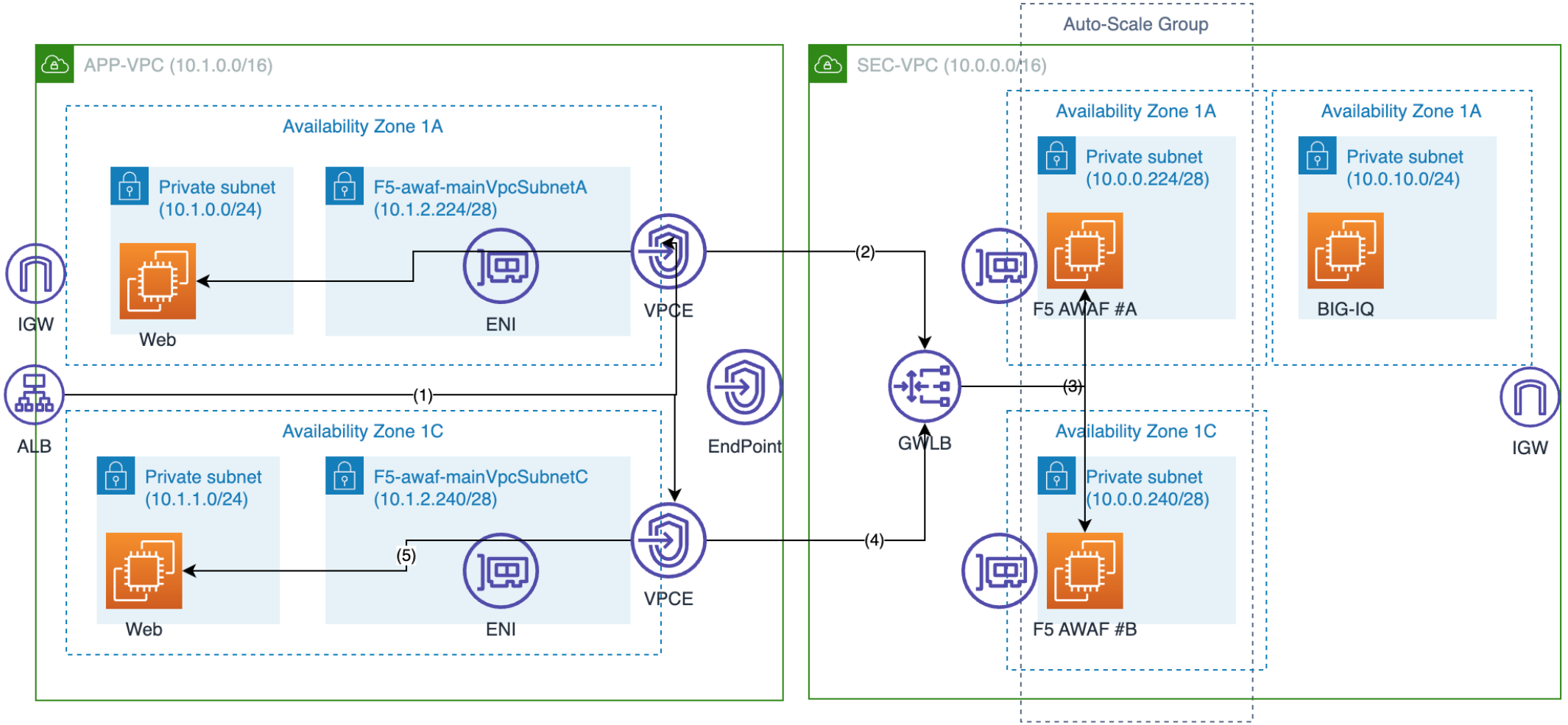
GWLB : 3rd Party 및 AZ 장애 failover 설계

- 기존 플로우 – 타겟 대상이 실패하면 ALB 및 NLB와 같은 로드 밸런서는 기존 플로우/세션을 종료하고 Reset 신호를 보냅니다. 그러나 GWLB는 투명한(transparent) bump-in-the-wire 디바이스기 때문에 fail-open 모드로 동작합니다. 즉, 기본적으로 Stateful의 기존 플로우는 시간이 초과되거나, 클라이언트에 의해 재설정될 때까지 실패한 대상과 계속 연결됩니다.

- 신규 플로우 – 헬스체크 설정(간격 및 임계값)에 따라 타겟 대상이 Unhealthy 플래그로 지정되면, GWLB는 신규 플로우를 정상 대상으로 다시 라우팅하기 전에 최대 50-60초의 지연을 추가합니다. 신규 플로우를 다시 라우팅하기 시작하는 최소 기간은 최대 70초입니다.
  - 헬스체크에 20초(최소 간격: 10초, 최소 임계값: 2)와 GWLB 백엔드가 감지하고 다시 라우팅하는 데 50초의 합계

GWLB : 3rd Party 장애 Failover 및 Auto-scaling 테스트 구성 환경

- 테스트 구성 환경



GWLB 비용

GWLB의 비용은 시간당 GWLB 엔드포인트당 과금과 시간당 GLCU별 과금의 합으로 계산

- 시간당 GWLB 엔드포인트 과금 : ($0.0125)
- 시간당 GLCU(GWLB 용량 단위) 과금 : ($0.004)

GLCU(Gateway Load balancer Capacity Unit)는 GWLB 용량 단위로, 아래 3가지 디멘션 중 가장 높은 사용율을 기준으로 산정

초당 신규 커넥션/플로우 (600개)

(분당 샘플링) 활성 커넥션/플로우 (60,000개)

시간당 쓰루풋 (1GB)

- https://aws.amazon.com/elasticloadbalancing/pricing/?nc1=h_ls

추가로 GWLBE에는 별도의 요금이 책정 및 청구됩니다. (AWS PrivateLink 요금 페이지)

GWLB 비용 계산 예시

예제 :

GWLB가 2개의 AZ에 배포되어서 총 4개의 GWLB-E(엔드포인트)에 서비스 제공 시,

각 GWLB-E는 초당 25개의 신규 커넥션을 수신하고, 각 연결은 4분간 유지되며, 처리된 바이트에 1KB를 소비하여, Gateway Load Balancer는 초당 100개의 새 연결을 수신하게 됩니다.

1. 시간당 GLCU(GWLB 용량 단위) 과금 :

- 새 커넥션 또는 흐름 수(초당): 각 GLCU는 초당 최대 600개의 새 커넥션을 제공합니다. GWLB가 **초당 100개의 새 커넥션을 수신하므로 이는 0.167GLCU(초당 100개의 새 커넥션/초당 600개의 새 커넥션)**에 해당

- 활성 커넥션 또는 흐름 수(분당): 각 GLCU는 분당 최대 60,000개의 활성 커넥션을 제공합니다. GWLB는 초당 100개의 새 커넥션을 수신하며 각 연결은 4분간 유지됩니다. 이는 **분당 24,000개 활성 커넥션, 즉 0.4 GLCU(분당 24,000개 활성 커넥션 / 분당 60,000개 활성 커넥션)**에 해당

- 처리된 바이트(시간당 GB): 각 GLCU는 1GB를 제공합니다. 각 커넥션이 대역폭을 기준으로 평균 1KB를 전송하므로, 이는 **시간당 0.36GB(초당 100개의 새 커넥션 * 커넥션당 1KB * 3,600초)으로 0.36 GLCU(시간당 0.36GB/시간당 1GB)**에 해당합니다.

이 예제에서는 활성 커넥션(0.4 GLCU)이 새 커넥션(0.167 GLCU) 및 처리된 바이트(0.36 GLCU) 보다 크므로, 이 사용량이 60분간 지속된다고 가정하면 총 요금은 시간당 **0.0016 USD(0.4 GLCU * GLCU당 0.004 USD**) 입니다.

GWLB 비용 계산 예시

2. 시간당 GWLB 엔드포인트 생성 과금과 1에서 계산한 시간당 GLCU 금액 합계 :

시간당 **0.0266 USD(각 AZ에서 시간당 0.0125 USD * 배포된 2개 AZ + 0.0016 USD/GLCU)**입니다.

3. GWLB 엔드포인트 비용 :

GWLB 엔드포인트별로 시간당 0.01 USD의 요금과 GB당 0.0035 USD의 데이터 전송 요금을 사용하여 월별 비용을 계산합니다. 그 결과 총 요금은 다음과 같습니다.

시간당 0.0413 USD(시간 요금 0.01 USD * GWLB 엔드포인트 4개 + GB당 0.0035 USD + GB당 0.36 USD) 입니다.

**** GWLB와 GWLB 엔드포인트의 총 합산 비용 :**

시간당 0.0679 USD(GWLB의 시간당 요금 0.0266 USD + GWLB 엔드포인트의 시간당 요금 0.0413 USD)

Q & A

Thank you!