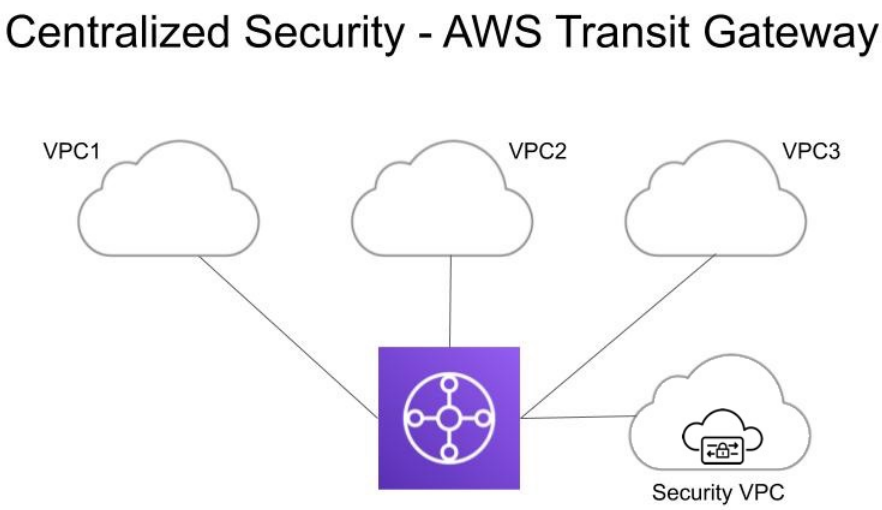
AWS

AWS 서비스 VPC 관리

AWS Transit Gateway를 사용하는 중앙 집중식 모드 구축의 경우, 멀티 클라우드 방어 게이트웨이은(는) 새 VPC에 구축됩니다. 이 VPC를 서비스 VPC라고 합니다. 서비스 VPC와 애플리케이션(스포크) VPC는 아래와 같이 허브 스포크 모델로 AWS Transit Gateway에 연결됩니다.



멀티 클라우드 방어은(는) 서비스 VPC 생성, AWS Transit Gateway 생성 (또는 재사용), 스포크 VPC 및 서비스 VPC를 Transit Gateway에 연결하는 것을 오케스트레이션합니다. 서비스 VPC 및 스포크 VPC 간의 라우팅을 업데이트합니다.

Note 다음 값이 올바르게 설정되지 않으면 트래픽이 서비스 VPC를 우회하여 다음에 의해 보호되지 않습니다.

- **AWS Terraform Provider**를 사용하여 Transit Gateway를 생성한 경우, `default_route_table_association` 및 `default_route_table_propagation` 속성을 비활성화로 설정해야 합니다.
- **AWS** 콘솔을 사용하여 Transit Gateway를 생성한 경우, 기본 연결 경로 테이블 및 기본 전파 경로 테이블 속성을 비활성화로 설정해야 합니다.
- 멀티 클라우드 방어 서비스 **VPC** 오케스트레이션을 사용하여 Transit Gateway를 생성한 경우 속성은 기본적으로 정확합니다.

AWS 서비스 VPC 생성

단계 **1** **Manage(**관리**)** > **Service VPCs/VNets(**서비스 **VPC/VNet)**를 클릭합니다.

단계 **2** **Create VPC/VNet(VPC/VNet** 생성**)**을 클릭합니다.

단계 **3** 서비스 VPC의 이름을 제공합니다(예 :멀티 클라우드 방어*-service-vpc1*).

단계 **4** AWS 계정을 선택합니다.

단계 **5** 서비스 VPC를 생성해야 하는 지역을 선택합니다(예: *us-east-1*).

단계 **6** 마스크가 최소 /25에서 최대 /16인 CIDR 블록을 제공합니다. Transit Gateway에 연결하려는 스포크 VPC CIDR과 겹치지 않는지 확인합니다(예: *172.16.0.0/16*).

단계 **7** **Availability Zones(**가용성 영역**)**를 선택합니다. HA를 위해서는 2개 이상의 AZ를 선택하는 것이 좋습니다(예: *us-east-1a* 및 *us-east-1b*).

단계 **8** **Transit Gateway**를 선택합니다. 또는 새로 생성합니다. 모든 종류의 보안 유형에 기존 Transit Gateway를 재사용할 수 있습니다.

단계 **9** 여러 AWS 계정에서 공유되는 Transit Gateway를 사용하려는 경우 **Auto accept shared attachments(**자동 수락 공유 첨부 파일**)**를 선택합니다.

단계 **10** **Save(**저장**)**를 클릭하여 서비스 VPC를 생성합니다.

Note

- 멀티 클라우드 방어은(는) 서비스 VPC가 생성될 때 다음과 같은 리소스를 생성합니다.
  - VPC
  - 각 AZ에 4개의 서브넷
  - 각 서브넷에 경로 테이블 1개
  - 보안 그룹 2개(관리 및 데이터 경로 트래픽)
- 각 보안 유형(인그레스, 이그레스, 이스트-웨스트)에 대해 서로 다른 서비스 VPC를 생성해야 합니다.
- Transit Gateway(서비스 VPC 생성 중에 생성/선택)는 다른 서비스 VPC에서 재사용할 수 있습니다.
- Transit Gateway를 검토합니다. 새 TTW를 생성하도록 선택한 경우 여기에 포함됩니다.
- 서비스 VPC에 대한 Transit Gateway 첨부 파일이 생성됩니다.
- Transit Gateway 경로 테이블이 생성되어 첨부 파일과 연결됩니다.
- AWS 게이트웨이 로드 밸런서)(GWLB)는 GWLB의 초기 구축 후 AZ 추가/제거를 지원하지 않습니다. AZ를 변경해야 하는 경우 서비스 VPC를 다시 구축해야 합니다.

허브 모드에서 스포크 VPC 관리

Transit Gateway로 서비스 VPC를 생성한 경우, 멀티 클라우드 방어은(는) Transit Gateway 및 서비스 VPC의 오케스트레이션을 처리합니다. 스포크 VPC에 대한 첨부 파일을 생성하고 Transit Gateway 라우팅 테이블을 관리할 수도 있습니다.

Note

- 서비스 VPC가 생성되고 상태가 **ACTIVE**가 될 때까지 기다렸다가 다음 단계를 진행하십시오.
- 멀티 클라우드 방어 게이트웨이은(는) 방금 생성한 서비스 VPC에서 나중에 구축할 수 있습니다.

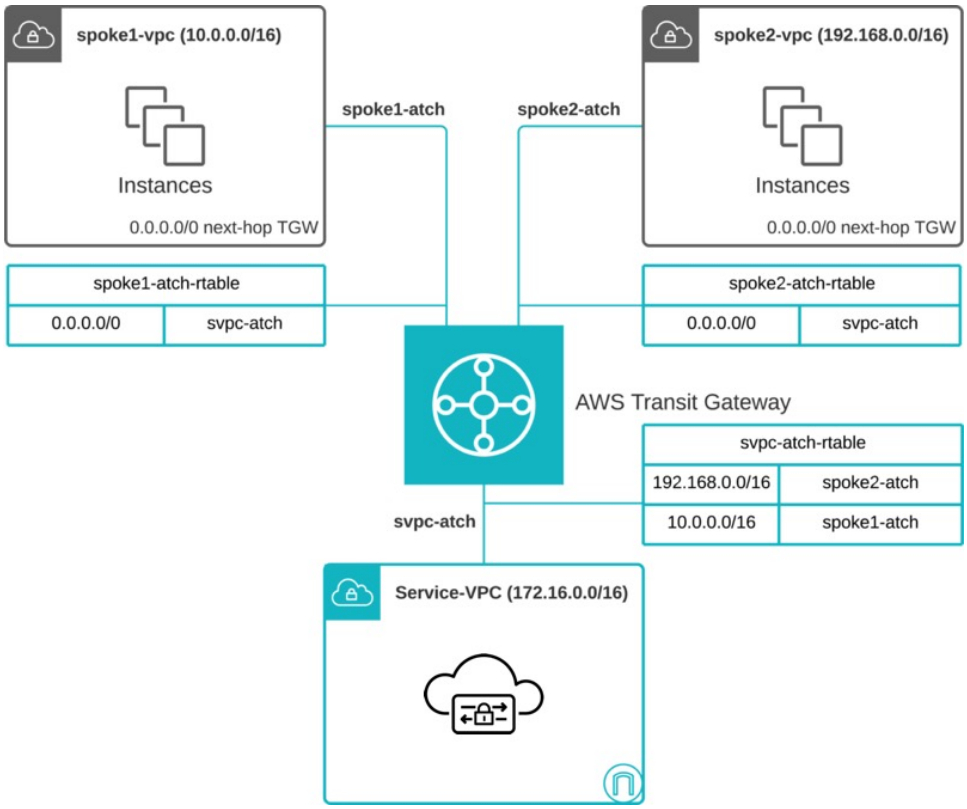
스포크 VPC를 보호하려면 서비스 VPC와 연결해야 합니다. 이를 통해 멀티 클라우드 방어은(는) 라우팅을 오케스트레이션하고 멀티 클라우드 방어에서 검사할 스포크 VPC의 트래픽에 대한 첨부 파일을 생성할 수 있습니다.

멀티 클라우드 방어 컨트롤러은(는) 스포크 VPC가 보안될 때 다음을 오케스트레이션합니다.

- 각 스포크 VPC에 대한 Transit Gateway VPC 첨부 파일을 생성합니다.
- 각 첨부 파일에 대해 Transit Gateway 경로 테이블을 추가하고 첨부 파일과 연결합니다.

- 스포크 VP와 연결된 TGW 경로 테이블에 기본 경로를 추가하여 서비스 VPC 첨부 파일로 이동합니다.

다음은 2개의 스포크 VPC 연결 후의 샘플 라우팅 설정입니다.



서비스 VPC 메뉴에서 스포크 VPC 추가

단계 1 **Manage(**관리**)** > **Service VPCs(**서비스 **VPC)**로 이동합니다.

단계 2 서비스 VPC를 선택하고 Manage Spoke VPCs(스포크 VPC 관리)를 클릭합니다.

단계 3 Transit Gateway가 생성된 현재 계정의 스포크 VPC에 대해 보호할 **Current Account VPCs(**현재 계정 **VPC)** 아래에 VPC를 추가합니다.

단계 4 드롭다운에서 VPC를 선택합니다. 이 테이블의 계정 및 지역은 변경할 수 없습니다. **Add(**추가**)**를 클릭하여 VPC를 더 추가합니다.

단계 5 다른 계정의 스포크 VPC에 대해 **External Account VPCs to Protect(**보호할 외부 계정 **VPC)** 테이블에 해당 VPC를 추가합니다. 계정, 지역 및 해당 지역에서 VPC를 선택하면 멀티 클라우드 방어이(가) 첨부 파일 초대를 자동으로 수락하도록 설정하므로 첨부 파일을 수락하기 위해 수동 단계를 수행할 필요가 없습니다.

VPC를 추가하기 전에 계정을 멀티 클라우드 방어 컨트롤러에 추가해야 합니다. 새 클라우드 계정을 멀티 클라우드 방어 컨트롤러에 추가하는 방법은 클라우드 계정 추가 섹션을 참조하십시오.

단계 6 경로 테이블 열에서 **View/Edit(**보기/편집**)** 링크를 클릭합니다.

단계 **7** Transit Gateway에 대한 기본 경로를 업데이트할 경로 테이블을 선택합니다.

단계 **8** (선택 사항) AWS ENI(Elastic Network Interface)를 배치할 서브넷을 선택하려면 TAW 첨부 서브넷을 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

재고 목록 메뉴에서 스포크 VPC 추가

단계 **1** **Manage(**관리**)** > **Cloud Accounts(**클라우드 계정**)** > **Inventory(**재고 목록**)**로 이동합니다.

단계 **2** 테이블 위에 있는 **VPC/VNets** 탭을 클릭합니다. 그러면 클라우드 계정의 모든 VPC가 나열됩니다. "Secured(보안)" 열에는 VPC의 보안 여부가 표시됩니다.

단계 **3** 오른쪽에 있는 **Secure(**보안**)** 버튼을 클릭합니다.

단계 **4** **Service VPC(**서비스 **VPC)**를 선택합니다.

단계 **5** **Route Table(**경로 테이블**)**을 선택하여 Transit Gateway 옆의 기본 경로를 업데이트합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

What to do next

(선택 사항) Transit Gateway 첨부를 위한 서브넷 선택, on page 5을(를) 맞춤 설정하도록 선택할 수 있습니다.

Transit Gateway 첨부를 위한 서브넷 선택

서비스 VPC 메뉴 또는 재고 목록 메뉴를 통해 중앙 집중식 모델에서 스포크 VPC를 보호하는 경우 멀티 클라우드 방어은(는) 서비스 VPC와 연결된 Transit Gateway에 VPC를 연결합니다. VPC를 Transit Gateway에 연결할 때 사용자는 ENI를 배치할 각 가용성 영역의 서브넷을 선택할 수 있습니다. 기본적으로 멀티 클라우드 방어은(는) Transit Gateway 연결에 대해 각 AZ에서 서브넷을 무작위로 선택합니다.

Transit Gateway 서브넷 선택을 사용자 지정하려면 서비스 VPC 메뉴에서 스포크 VPC 추가, on page 4 또는 재고 목록 메뉴에서 스포크 VPC 추가를 참조하십시오.

중앙 집중식 모드에서 스포크 VPC 관리

중앙 집중식 모드로 구축한 경우 게이트웨이는 역방향 프록시로 작동합니다. 인터넷 사용자는 멀티 클라우드 방어 게이트웨이을(를) 통해 애플리케이션에 액세스합니다. 멀티 클라우드 방어 게이트웨이에서 프록시 대상으로 백엔드 대상(원래 애플리케이션)을 구성합니다. 프록시를 사용하면, 멀티 클라우드 방어은(는) TLS 트래픽을 암호 해독하고 심층 패킷 검사를 수행할 수 있습니다. 백엔드/대상에 대해 프록시된 트래픽은 일반 텍스트 HTTP, HTTPS, TCP 또는 TLS로 전송될 수 있습니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** **Add Gateway(**게이트웨이 추가**)**를 클릭합니다.

단계 **3** 이전에 생성한 계정을 선택합니다.

단계 **4** **Next(**다음**)**를 클릭하고 적절한 정보를 활성화합니다.

- **Instance Type(**인스턴스 유형**)** - 클라우드 서비스 제공자의 유형을 선택합니다. 사용 중인 클라우드 서비스 제공자에 따라 인스턴스의 여러 변형이 있을 수 있습니다.
- **Gateway Tpe(**게이트웨이 **Tpe)** - 자동 확장.
- **Minimum Instances(**최소 인스턴스**)** - 구축하려는 최소 인스턴스 수를 선택합니다.
- **Maximum Instances(**최대 인스턴스**)** - 구축하려는 최대 인스턴스 수를 선택합니다. 이는 각 가용성 영역에서 자동 확장에 사용되는 최대 수입니다.
- **HealthCheck Port(HealthCheck** 포트**)** - 기본값은 65534입니다. 멀티 클라우드 방어 로드 밸런서에서 인스턴스의 상태를 확인하는 데 사용하는 포트 번호입니다. 인스턴스에 할당된 데이터 경로 보안 그룹은 이 포트에서 트래픽을 허용해야 합니다.
- (선택 사항) **Packet Capture Profile(**패킷 캡처 프로파일**)** - 위협 및 플로우 PCAP에 대한 패킷 캡처 프로파일입니다.
- (선택 사항) **Diagnostics Profile(**진단 프로파일**)** - 기술 지원 정보를 저장하는 데 사용되는 진단 프로파일입니다.
- (선택 사항) **Log Profile(**로그 프로파일**)** - 이벤트/로그를 SIEM으로 전달하는 데 사용되는 로그 전달 프로파일입니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** 다음 매개변수를 제공합니다.

- **Security(**보안**)** - 인그레스
- **Gateway Image(**게이트웨이 이미지**)** - 구축할 이미지.
- **Policy Ruleset(**정책 규칙 집합**)** - 이 게이트웨이와 연결할 정책 규칙 집합을 선택합니다.
- **Region(**지역**)** - 이 게이트웨이를 구축할 지역을 선택합니다.
- **VPC** - 멀티 클라우드 방어 게이트웨이이(가) 구축된 VPC를 선택합니다.
- **Key Pair(**키 쌍**)** - 이 게이트웨이와 연결할 키 쌍을 선택합니다.
- **IAM Role for Gateway(**게이트웨이의 **IAM** 역할**)** - 이 게이트웨이와 연결할 IAM 역할을 선택합니다.
- **Mgmt. Security Group(**관리 보안 그룹**)** - 관리 인터페이스와 연결할 보안 그룹을 선택합니다.
- **Datapath Security Group(**데이터 경로 보안 그룹**)** - 데이터 경로 인터페이스와 연결할 보안 그룹을 선택합니다.
- **EBS Encryption(EBS** 암호화**)** - 게이트웨이 인스턴스에 대해 EBS 암호화를 활성화합니다. 활성화된 경우 사용자는 **AWS** 관리형 **CMK** 또는 고객 관리형 암호화 키를 선택합니다. 고객 관리 암호화 키의 경우 KMS 키 ARN을 제공해야 합니다.

단계 **7** **Availability Zone(**가용성 영역**)**, **Mgmt Subnet(**관리 서브넷**)** 및 **Datapath Subnet(**데이터 경로 서브넷**)**을 선택합니다. 사용 가능한 서브넷은 위에서 선택한 VNet을 기반으로 합니다. 고가용성을 위해 게이트웨이 인스턴스를 여러 가용성 영역에 구축할 수 있습니다. 더하기 버튼을 클릭하여 새 가용성 영역을 추가하고 선택한 영역에 대한 매개변수를 선택합니다.

단계 **8** **Next(**다음**)**를 클릭합니다. 검토 페이지에 선택한 모든 매개변수의 상세정보가 표시됩니다. 사용 가능한 리소스를 검토하고 초과된 AWS 제한에 대한 정보를 확인합니다.

단계 **9** 마침을 클릭합니다. 게이트웨이 구축이 시작되고 게이트웨이가 **ACTIVE** 상태가 될 때까지 약 5~7분 정도 걸립니다.

Note AWS 콘솔에서 EC2 인스턴스 페이지를 보고 게이트웨이 인스턴스가 생성되었는지 확인합니다. 인스턴스에는 멀티 클라우드 방어(으)로 시작하는 이름 태그가 있습니다.

Check Load Balancers(로드 밸런서 확인**)** 섹션으로 이동하여 인터넷을 향한 네트워크 로드 밸런서가 생성되었는지 확인합니다. 아직 리스너 또는 대상 그룹이 없습니다. 리스너 포트 및 백엔드 애플리케이션이 있는 서비스를 추가할 때 리스너 및 대상 그룹(EC2 멀티 클라우드 방어 게이트웨이 인스턴스를 대상)이 생성됩니다.

고급 설정: 전역 가속기

멀티 클라우드 방어은(는) 멀티 클라우드 방어 게이트웨이 인스턴스 전체에서 트래픽을 로드 밸런싱하는 하나 이상의 AWS 글로벌 액셀러레이터 세트와 통합하여 인그레스 포인트로 사용할 수 있습니다. 이는 인그레스 게이트웨이가 구축될 때 멀티 클라우드 방어에서 생성 및 관리하는 AWS 네트워크 로드 밸런서와 유사하지만, 애플리케이션 및 워크로드를 보호하기 위해 인그레스 게이트웨이에 대체 인그레스 포인트를 제공합니다.

가속기를 사용하는 경우, 전역 가속기의 리스너 엔드포인트 그룹을 관리하여 엔드포인트 그룹에 활성 게이트웨이 인스턴스 집합이 있는지 확인합니다. 클라이언트 IP 주소는 전역 가속기를 통과할 때 유지됩니다.

멀티 클라우드 방어 인그레스 게이트웨이에 대한 가속기.

멀티 클라우드 방어을(를) 전역 가속기와 통합하려면 사용자는 먼저 AWS 내에 전역 가속기를 생성하고, 원하는 리스너를 정의한 다음 빈 엔드포인트 그룹(또는 기존 멀티 클라우드 방어 인그레스 게이트웨이 인스턴스를 포함하는 엔드포인트 그룹)을 생성해야 합니다. AWS 리소스가 있으면 글로벌 가속기와 통합하도록 멀티 클라우드 방어 인그레스 게이트웨이를 구성할 수 있습니다.

매개변수	설명
전역 가속기	게이트웨이에 연결할 전역 가속기를 선택합니다.
리스너 이름	리스너의 식별 이름입니다. 이 이름은 멀티 클라우드 방어에만 존재합니다.
리스너	전역 가속기의 리스너입니다.

매개변수	설명
엔드포인트 그룹 ARN	멀티 클라우드 방어은(는) 리스너가 선택되면 엔드포인트 그룹 ARN을 자동으로 선택합니다.

Note

- AWS 전역 가속기 통합이 활성화된 경우에도 AWS 네트워크 로드 밸런서는 게이트웨이 구축의 일부로 구축됩니다.
- AWS 전역 가속기 리스너에서 엔드포인트 그룹을 구성할 때는 상태 검사 포트로 TCP/65534를 할당하는 것이 가장 좋습니다. TCP/65534에 응답하여 AWS 네트워크 로드 밸런서 및 AWS 전역 로드 밸런서의 상태를 알리도록 멀티 클라우드 방어 게이트웨이을(를) 구성합니다. 상태를 AWS 전역 가속기에 알리는 데 동일한 포트를 사용할 수 있습니다.

AWS 중앙 집중식 이그레스/이스트-웨스트 보호

멀티 클라우드 방어 게이트웨이은(는) VPC 내부에서 실행되는 애플리케이션의 발신 트래픽을 보호하기 위해 단일 VPC에 구축됩니다. 이 게이트웨이는 전달 프록시 역할을 합니다. SNI 확장 헤더가 있는 HTTP 또는 TLS 애플리케이션의 경우 멀티 클라우드 방어 게이트웨이은(는) 투명 전달 프록시로 작동합니다. 애플리케이션은 변경 없이 인터넷에 액세스합니다. 멀티 클라우드 방어은(는) 트래픽을 가로채고 프록시된 트래픽으로 간주합니다. 인터넷에 대한 새 세션이 생성됩니다. 클라이언트 애플리케이션에서 TLS 트래픽과 인증서를 신뢰하려면 멀티 클라우드 방어에 신뢰할 수 있는 루트/중간 인증서를 구성하고 모든 클라이언트 애플리케이션 인스턴스에 루트 인증서를 설치해야 합니다.

단계 **1** **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다.

단계 **2** **Add Gateway(**게이트웨이 추가**)**를 클릭합니다.

단계 **3** 이전에 생성한 계정을 선택합니다.

단계 **4** **Next(**다음**)**를 클릭하고 다음 매개변수를 입력합니다.

-
- **Instance Type(**인스턴스 유형**)** - 클라우드 서비스 제공자의 유형을 선택합니다. 사용 중인 클라우드 서비스 제공자에 따라 인스턴스의 여러 변형이 있을 수 있습니다.
- **Gateway Tpe(**게이트웨이 **Tpe)** - 자동 확장.
- **Minimum Instances(**최소 인스턴스**)** - 구축하려는 최소 인스턴스 수를 선택합니다.
- **Maximum Instances(**최대 인스턴스**)** - 구축하려는 최대 인스턴스 수를 선택합니다. 이는 각 가용성 영역에서 자동 확장에 사용되는 최대 수입니다.
- **HealthCheck Port(HealthCheck** 포트**)** - 기본값은 65534입니다. 멀티 클라우드 방어 로드 밸런서에서 인스턴스의 상태를 확인하는 데 사용하는 포트 번호입니다. 인스턴스에 할당된 데이터 경로 보안 그룹은 이 포트에서 트래픽을 허용해야 합니다.

- (선택 사항) **Packet Capture Profile(**패킷 캡처 프로파일**)** - 위협 및 플로우 PCAP에 대한 패킷 캡처 프로파일입니다.
- (선택 사항) **Diagnostics Profile(**진단 프로파일**)** - 기술 지원 정보를 저장하는 데 사용되는 진단 프로파일입니다.
- (선택 사항) **Log Profile(**로그 프로파일**)** - 이벤트/로그를 SIEM으로 전달하는 데 사용되는 로그 전달 프로파일입니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** 다음 매개변수를 제공합니다.

- **Security(**보안**)** - 이그레스.
- **Gateway Image(**게이트웨이 이미지**)** - 구축할 이미지.
- **Policy Ruleset(**정책 규칙 집합**)** - 이 게이트웨이와 연결할 정책 규칙 집합을 선택합니다.
- **Region(**지역**)** - 이 게이트웨이를 구축할 지역을 선택합니다.
- **VPC** - 멀티 클라우드 방어 게이트웨이이(가) 구축된 VPC를 선택합니다.
- **Key Pair(**키 쌍**)** - 이 게이트웨이와 연결할 키 쌍을 선택합니다.
- **IAM RoleforGateway** - 이 게이트웨이와 연결할 IAM 역할을 선택합니다.
- **Mgmt. Security Group(**관리 보안 그룹**)** - 관리 인터페이스와 연결할 보안 그룹을 선택합니다.
- **Datapath Security Group(**데이터 경로 보안 그룹**)** - 데이터 경로 인터페이스와 연결할 보안 그룹을 선택합니다.
- **EBS Encryption(EBS** 암호화**)** - 게이트웨이 인스턴스에 대해 EBS 암호화를 활성화합니다. 활성화된 경우 사용자는 **AWS** 관리형 **CMK** 또는 고객 관리형 암호화 키를 선택합니다. 고객 관리 암호화 키의 경우 **KMS** 키 **ARN**을 제공해야 합니다.

단계 **7** **Availability Zone(**가용성 영역**)**, **Mgmt Subnet(**관리 서브넷**)** 및 **Datapath Subnet(**데이터 경로 서브넷**)**을 선택합니다. 사용 가능한 서브넷은 위에서 선택한 VNet을 기반으로 합니다. 고가용성을 위해 게이트웨이 인스턴스를 여러 가용성 영역에 구축할 수 있습니다. 더하기 버튼을 클릭하여 새 가용성 영역을 추가하고 선택한 영역에 대한 매개변수를 선택합니다.

단계 **8** **Next(**다음**)**를 클릭합니다. 검토 페이지에 선택한 모든 매개변수의 상세정보가 표시됩니다. 사용 가능한 리소스를 검토하고 초과된 AWS 제한에 대한 정보를 확인합니다.

단계 **9** 마침을 클릭합니다. 게이트웨이 구축이 시작되고 게이트웨이가 **ACTIVE** 상태가 될 때까지 약 5~7분 정도 걸립니다.

Note

- AWS Console **Load Balancers(**로드 밸런서**)** 섹션에서 내부 네트워크 로드 밸런서가 생성되었는지 확인합니다. 아직 리스너 또는 대상 그룹이 없습니다. 리스너 포트 및 백엔드 애플리케이션이 있는 서비스를 추가할 때 리스너 및 대상 그룹(EC2 멀티 클라우드 방어 게이트웨이 인스턴스를 대상)이 생성됩니다.
- AWS 콘솔에서 **EC2** 인스턴스 페이지를 확인하고 게이트웨이 인스턴스가 생성되었는지 확인합니다. 인스턴스에는 멀티 클라우드 방어(으)로 시작하는 이름 태그가 있습니다. 게이트웨이 인스턴스와 함께 다른 헬퍼/지원 인스턴스가 생성됩니다. 이를 **NAT** 인스턴스라고 합니다. 게이트웨이가 생성되어 **ACTIVE** 상태가 된 후에는 애플리케이션 서브넷과 연결된 경로 테이블에서 경로를 추가하여 기본 경로의 다음 홉을 NAT 인스턴스의 인터페이스로 사용할 수 있습니다. 트래픽이 애플리케이션 서브넷에서 나갈 때 NAT 인스턴스에 도달합니다. 패킷의 대상 IP가 내부 네트워크 로드 밸런서의 IP로 변경됩니다. 이렇게 하면 트래픽이 게이트웨이 인스턴스에 도달합니다. 게이트웨이는 SNI 또는 HTTP 호스트 헤더를 검사하여 대상 주소를 찾고 패킷을 전송합니다. 애플리케이션이 TLS를 통해 통신할 때 게이트웨이는 Client Hello가 게이트웨이에 도달할 때까지 기다린 다음 대상에 대해 새 연결을 생성합니다(SNI 필드에 정의됨). 인터넷 서버에서 발신되는 수신 인증서는 멀티 클라우드 방어 게이트웨이에 설치된 루트/중간 인증서로 가장하고 애플리케이션으로 전송합니다.