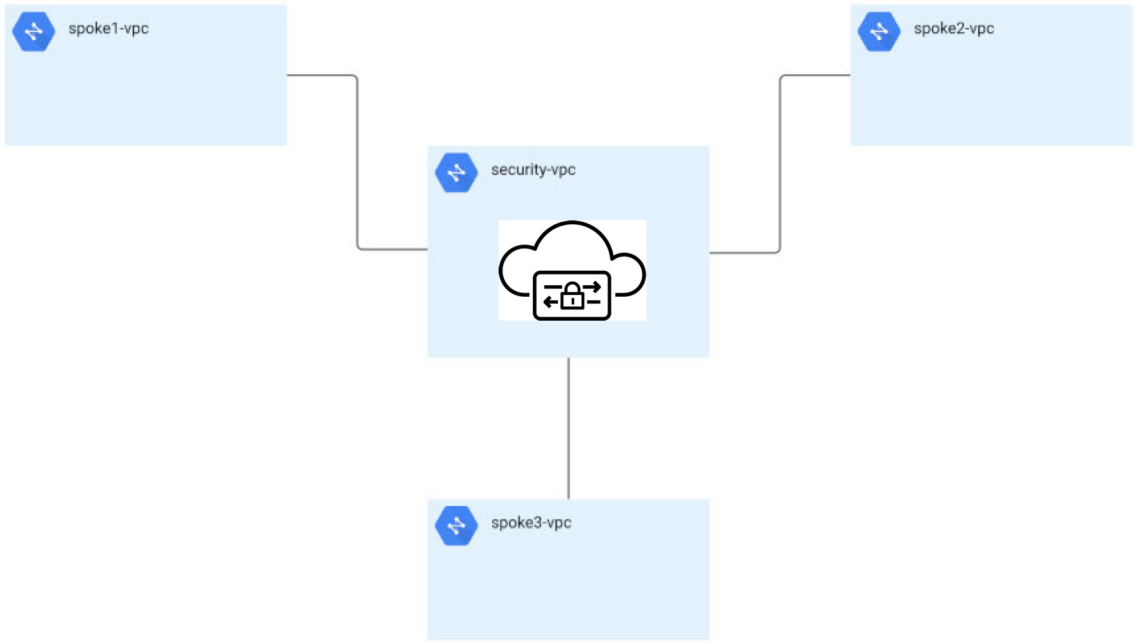
GCP

서비스 GCP

GCP 서비스 VPC

중앙 집중식 구축의 경우 멀티 클라우드 방어 게이트웨이이(가) 새 VPC에 구축됩니다. 이 VPC를 서비스 VPC라고 하며 다른 스포크(애플리케이션) VPC와 피어링을 통해 아래에 나와 있는 허브 및 스포크 모델을 생성합니다.



멀티 클라우드 방어은(는) 서비스 VPC의 생성과 스포크 VPC와의 피어링을 오케스트레이션합니다. 또한 멀티 클라우드 방어은(는) 스포크 VPC의 라우팅 테이블을 업데이트하여 검사를 위해 트래픽을 서비스 VPC로 라우팅하는 기능도 제공합니다. 스포크 VPC에서 멀티 클라우드 방어을(를) 사용하여 라우팅을 변경하는 방법에 대한 지침은 허브 모드에서 스포크 VPC 관리(보호)를 참조하십시오.

서비스 VPC 생성

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

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

단계 3 입력 매개변수 값:

매개변수	설명
이름	서비스 VPC에 이름을 할당합니다.
CSP 계정	서비스 VPC를 생성할 GCP 프로젝트를 선택합니다.
지역	서비스 VPC를 구축할 GCP 지역입니다.
데이터 경로 CIDR 블록	멀티 클라우드 방어 게이트웨이 데이터 경로 서비스 VPC에 대한 CIDR 블록. 이 CIDR 블록은 스포크(애플리케이션) VPC의 주소 범위와 중복되지 않아야 합니다.
관리 CIDR 블록	멀티 클라우드 방어 게이트웨이 관리 서비스 VPC에 대한 CIDR 블록입니다. 이 CIDR 블록은 스포크(애플리케이션) VPC의 주소 범위와 중복되지 않아야 합니다.
가용성 영역	멀티 클라우드 방어에서는 복원력을 위해 2개 이상의 가용성 영역을 선택할 것을 권장합니다.

Note

- 서비스 VPC는 다음으로 구성됩니다.
  - 2개의 VPC - 관리용 1개, 데이터 경로 1개
  - 방화벽 규칙 4개 - 관리용 2개, 데이터 경로 2개(인그레스 및 이그레스)
- 서비스 VPC CIDR은 스포크 VPC와 중복되지 않아야 합니다.

허브 모드에서 스포크 VPC 관리(보호)

멀티 클라우드 방어에서는 서비스 VPC 생성을 오케스트레이션하고 스포크 VPC에 대한 VPC 피어링도 생성합니다. 멀티 클라우드 방어은(는) 스포크 VPC에 대한 라우트 테이블 변경을 수행할 수 있어 검사를 위해 트래픽이 멀티 클라우드 방어 게이트웨이(으)로 라우팅됩니다. 이 멀티 클라우드 방어 오케스트레이션을 사용하면 워크로드를 매우 쉽게 구축하고 보호할 수 있습니다.

Note 서비스 VPC가 생성될 때까지 몇 분 기다렸다가 상태가 **ACTIVE** 상태로 전환될 때까지 기다렸다가 다음 단계를 진행하십시오.

스포크 VPC를 보호하려면 스포크 VPC와 서비스 VPC 사이에 VPC 피어링을 생성해야 합니다. 이를 통해 멀티 클라우드 방어은(는) 스포크 VPC의 라우팅 변경을 오케스트레이션하여 트래픽이 검사를 위해 멀티 클라우드 방어 게이트웨이(으)로 전송되도록 할 수 있습니다.

보호된 VPC를 활성화하는 경우, 멀티 클라우드 방어 컨트롤러은(는) 다음을 오케스트레이션합니다.

- 멀티 클라우드 방어 서비스 VPC(데이터 경로)와 스포크 VPC 간에 VPC 피어링 생성
- 스포크 트래픽을 멀티 클라우드 방어 게이트웨이(으)로 리디렉션할 기본 경로 추가/업데이트

이 구성을 만드는 두 가지 방법이 있습니다.

- 서비스 VPC 메뉴에서 스포크 VPC 추가, on page 3
- 재고 목록 메뉴에서 스포크 VPC 추가, on page 3

서비스 **VPC** 메뉴에서 스포크 **VPC** 추가

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

단계 **2** Service VNet(서비스 VNet)을 선택하고 **Actions(**작업**)** > **Manage Spoke VPC/VNet(**스포크 **VPC/VNet** 관리**)**을 클릭합니다.

단계 **3** 보호할 모든 스포크 VPC를 스포크 테이블에 추가합니다.

단계 **4** Route Tables(경로 테이블) 열에서 View/Edit(보기/편집) 링크를 클릭합니다.

단계 **5** 검사를 위해 멀티 클라우드 방어 게이트웨이을(를) 가리키도록 기본 경로를 업데이트하려면 **Send Traffic via** 멀티 클라우드 방어 게이트웨이**(**을 통해 트래픽 전송**)** 확인란을 선택합니다.

단계 **6** **Update routes(**경로 업데이트**)**를 클릭합니다.

단계 **7** **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** VPC/VNets를 클릭합니다. 그러면 클라우드 계정의 모든 VPC가 나열됩니다.

단계 **3** VPC를 보호하려면 **Secure(**보안**)** 버튼을 클릭합니다.

단계 **4** Service VPC(서비스 VPC)를 선택합니다.

단계 **5** **"Send Traffic via** 멀티 클라우드 방어 게이트웨이**(**을**(**를**)** 통해 트래픽 전송**)"** 확인란을 선택합니다. 멀티 클라우드 방어에 대한 스포크 VPC의 기본 경로가 구성됩니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

GCP 중앙 집중식 인그레스 보호

멀티 클라우드 방어 게이트웨이은(는) 역방향 프록시 역할을 하여 애플리케이션을 보호하기 위해 VPC에 구축됩니다. 사용자는 멀티 클라우드 방어 게이트웨이을(를) 통해 애플리케이션에 액세스합니다. 백엔드 애플리케이션은 멀티 클라우드 방어 게이트웨이에 프록시 대상으로 설정됩니다. 역방향 프록시 기능을 사용하려면 멀티 클라우드 방어이(가) TLS 트래픽을 암호 해독하고 심층 패킷 검사를 수행해야 합니다. 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** 해당되는 경우 게이트웨이 정보를 입력합니다.

- **Instance Type(**인스턴스 유형**)** - 클라우드 서비스 제공자의 유형을 선택합니다. 사용 중인 클라우드 서비스 제공자에 따라 인스턴스의 여러 변형이 있을 수 있습니다.
- **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.
- (선택 사항) **Disk Encryption(**디스크 암호화**) - GCPmanaged encryption(GCP** 관리 암호화**)**또는 **Customermanaged encryption key(C**고객 관리 암호화 키**)**를 선택합니다. 고객 관리 암호화 키의 경우, 사용자는 암호화 키의 리소스 ID를 입력해야 합니다.

단계 **5**

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 다음 매개변수를 입력합니다.

- **Type(**유형**)** - 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.
- **Gateway Service Account Email(**게이트웨이 서비스 계정 이메일**)** - 멀티 클라우드 방어 게이트웨이 서비스 계정 이메일을 입력합니다. 서비스 계정에 필요한 IAM 역할(`Secret Manager Secret Accessor(Secret Manager 암호 접근자)` 및 `Storage Object Creator(스토리지 개체 생성자)`)이 있는지 확인합니다.
- **Datapath VPC(**데이터 경로 **VPC)** - 게이트웨이의 데이터 경로 인터페이스와 연결할 VPC를 선택합니다.
- **Datapath Network Tag(**데이터 경로 네트워크 태그**)** - 데이터 경로 VPC에 있는 게이트웨이의 네트워크 인터페이스에 할당된 태그입니다.
- **Management VPC(**관리 **VPC)** - 게이트웨이의 관리 인터페이스와 연결할 VPC를 선택합니다.
- **Management Network Tag(**관리 네트워크 태그**)** - 관리 VPC에 있는 게이트웨이의 네트워크 인터페이스에 할당된 태그입니다.

단계 **8** **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 **9** 멀티 클라우드 방어 게이트웨이 구축이 **Active(**활성**)** 상태가 되는 데 몇 분 정도 걸립니다.

GCP 중앙 집중식 이그레스/이스트-웨스트 보호

멀티 클라우드 방어 게이트웨이은(는) VPC 내부의 아웃바운드 및 이스트-웨스트 트래픽을 보호하기 위해 VPC에 구축됩니다. SNI 확장 헤더가 있는 HTTP 또는 TLS 애플리케이션의 경우 멀티 클라우드 방어 게이트웨이은(는) 투명 전달 프록시로 작동합니다. 멀티 클라우드 방어에서는 아웃바운드 세션을 종료하고, VPC 내부의 클라이언트를 대신하여 요청을 프록시합니다. 이 암호 해독/암호화 작업이 작동하려면 신뢰할 수 있는 루트/중간 인증서를 멀티 클라우드 방어 게이트웨이 및 클라이언트 애플리케이션 인스턴스에 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 클릭합니다.

- **Instance Type(**인스턴스 유형**)** - 클라우드 서비스 제공자의 유형을 선택합니다. 사용 중인 클라우드 서비스 제공자에 따라 인스턴스의 여러 변형이 있을 수 있습니다.

- **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.
- **Disk Encryption(**디스크 암호화**)** - **GCPmanaged encryption(GCP** 관리 암호화**)** 또는 **Customermanaged encryption key(**고객 관리 암호화 키**)**를 선택합니다. 고객 관리 암호화 키의 경우, 사용자는 암호화 키의 리소스 ID를 입력해야 합니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** 다음 매개변수를 제공합니다.

- **Type(**유형**)** - 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.
- **Gateway Service Account Email(**게이트웨이 서비스 계정 이메일**)** - 멀티 클라우드 방어 게이트웨이 서비스 계정 이메일을 입력합니다. 서비스 계정에 필요한 IAM 역할(`Secret Manager Secret Accessor(Secret Manager 암호 접근자)` 및 `Storage Object Creator(스토리지 개체 생성자)`)이 있는지 확인합니다.
- **Datapath VPC(**데이터 경로 **VPC)** - 게이트웨이의 데이터 경로 인터페이스와 연결할 VPC를 선택합니다.
- **Datapath Network Tag(**데이터 경로 네트워크 태그**)** - 데이터 경로 VPC에 있는 게이트웨이의 네트워크 인터페이스에 할당된 태그입니다.
- **Management VPC(**관리 **VPC)** - 게이트웨이의 관리 인터페이스와 연결할 VPC를 선택합니다.
- **Management Network Tag(**관리 네트워크 태그**)** - 관리 VPC에 있는 게이트웨이의 네트워크 인터페이스에 할당된 태그입니다.

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** 게이트웨이 구축이 **Active(**활성**)** 상태가 되는 데 몇 분 정도 걸립니다.