멀티 클라우드 방어 마법사를 사용하여 설정

멀티 클라우드 방어 컨트롤러에서는 멀티 클라우드 방어를 구축 및 관리할 수 있는 SaaS 제공 중앙 집중식 컨트롤 플레인 및 해당 보안 정책을 제공합니다.

설정은 다음과 같은 일련의 간단한 단계를 통해 멀티 클라우드 방어 보안을 설정하는 프로세스를 사용자에게 안내합니다.

- 어카운트 연결- 이 프로세스에서는 클라우드 서비스 제공자 어카운트를 멀티 클라우드 방어에 온보딩하고 어카운트와 관련된 지역 및 추가 인벤토리 목록 및 자산을 검색합니다.
- 트래픽 가시성 활성화 - 쉬운 설정 방법을 사용하면 로그 수집을 활성화하여 트래픽 흐름을 파악합니다.
- 어카운트 보호 - 이 절차를 수행하면 보유한 클라우드 어카운트에 따라 VNET 또는 VPC를 쉽게 설정하고 멀티 클라우드 방어 게이트웨이로 환경을 보호할 수 있습니다.

- 클라우드 어카운트 연결, on page 1
- 트래픽 가시성 활성화, 8 페이지
- 어카운트 보안, 9 페이지

클라우드 어카운트 연결

첫 번째 단계는 하나 이상의 클라우드 어카운트를 온보딩하는 것입니다. 멀티 클라우드 방어 컨트롤러에서 인벤토리 목록을 검색하고 트래픽 및 로그를 활성화하고 보안 구축을 오케스트레이션하고 정책을 생성 및 관리하여 각 계정과 상호 작용할 수 있습니다.

다음 절차를 사용하여 클라우드 서비스 제공자 계정을 멀티 클라우드 방어 컨트롤러에 연결합니다.

AWS 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어의 쉬운 설정 마법사를 통해 AWS 구독에 연결합니다.

시작하기 전에

- 활성 AWS(Amazon Web Services) 어카운트가 있어야 합니다.

- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어를 활성화해야 합니다.

참고 멀티 클라우드 방어 컨트롤러 버전 23.10은 멀티 클라우드 방어 게이트웨이 버전 23.04 이상을 사용하는 경우 AWS EC2 인스턴스에서 기본적으로 IMDSv2를 사용합니다. IMDSv1과 IMDSv2의 차이점에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.

단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.

단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup(**설정**)**을 클릭합니다.

단계 **4** **Connect Account(**어카운트 연결**)**를 선택합니다.

단계 **5** AWS 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) **Launch Stack(**스택 실행**)**을 클릭하여 CloudFormation 템플릿을 다운로드하고 구축합니다. 이렇게 하면 템플릿을 구축할 수 있는 다른 탭이 열립니다. AWS에 로그인해야 합니다.

b) CloudFormation 템플릿의 CloudFormation 스택 출력에서 컨트롤러 IAM 역할 ARN을 복사하여 붙여넣습니다.

c) 멀티 클라우드 방어 컨트롤러 쉬운 설정 모달에서 **AWS Account Number(AWS** 계정 번호**)**를 입력합니다. 이 번호는 CloudFormation 템플릿의 출력 값 **Current Account**에서 찾을 수 있습니다.

d) 멀티 클라우드 방어 컨트롤러에 계정에 할당될 **Account Name(**계정 이름**)**을 입력합니다.

e) (선택 사항) 계정 설명을 입력합니다.

f) 외부 **ID**를 입력합니다. IAM 역할의 신뢰 정책에 대한 임의의 문자열입니다. 이 값은 생성된 컨트롤러 IAM 역할에서 사용됩니다. 외부 ID를 편집하거나 다시 생성할 수 있습니다.

g) **Controller IAM Role(**컨트롤러 **IAM** 역할**)**을 입력합니다. 이 역할은 CFT(CloudFormation Template) 구축 중에 멀티 클라우드 방어 컨트롤러에 대해 생성되는 IAM 역할입니다. CFT 스택에서 출력 값 MCDControllerRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.

h) **Inventory Monitor Role(**인벤토리 목록 모니터 역할**)**을 입력합니다. 이 역할은 CFT 구축 중에 멀티클라우드 방어 인벤토리 목록에 대해 생성된 IAM 역할입니다. CFT 스택에서 출력 값 MCDInventoryRoleArn을 찾습니다. 다음과 유사해야 합니다: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

단계 **7** **Next(**다음**)**를 클릭합니다. 계정이 멀티 클라우드 방어 컨트롤러에 온보딩됩니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

Azure 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어 컨트롤러의 쉬운 설정 마법사를 통해 Azure 구독에 연결합니다.

시작하기 전에

- 활성 Azure 구독이 있어야 합니다.
- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어을(를) 활성화해야 합니다.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.

단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.

단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup(**설정**)**을 클릭합니다.

단계 **4** **Connect Account(**어카운트 연결**)**를 선택합니다.

단계 **5** Azure 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) 링크를 클릭하여 Bash 모드에서 Azure Cloud Shell을 엽니다.
b) Azure 계정 모달에서 **Copy(**복사**)**를 클릭하여 온보딩 스크립트를 복사하고 1단계에서 연 Bash 쉘에서 실행합니다.
c) Azure 계정 모달에서 이 Azure 계정의 이름을 제공합니다. 이 이름은 Azure 구독 이름과 동일하게 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러 계정 페이지에만 표시됩니다.
d) (선택 사항) 구독에 대한 설명을 제공합니다.
e) 테넌트 ID라고도 하는 디렉터리 **ID**를 입력합니다.
f) 온보딩 중인 구독의 구독 **ID**를 입력합니다.
g) 온보딩 스크립트에서 생성한 애플리케이션 **ID**(클라이언트 ID라고도 함)를 입력합니다.
h) **Client Secret(**클라이언트 암호**)**(암호 ID라고도 함)을 입력합니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

Google Cloud 플랫폼 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어 컨트롤러의 간편한 설정 마법사를 사용하여 GCP 프로젝트를 계정으로 온보딩합니다.

시작하기 전에

- 액티브 GCP(Google Cloud Platform) 프로젝트가 있어야 합니다.
- GCP 프로젝트 내에서 VPC, 서브넷, 서비스 어카운트를 생성하는 데 필요한 권한이 있어야 합니다. 자세한 내용은 GCP 문서를 참조하십시오.
- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어을(를) 활성화해야 합니다.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.

단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.

단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup(**설정**)**을 클릭합니다.

단계 **4** **Connect Account(**어카운트 연결**)**를 선택합니다.

단계 **5** GCP 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) **Cloud Platform Cloud Shell(**클라우드 플랫폼 클라우드 쉘**)**을 클릭하여 클라우드 쉘을 시작합니다.

b) 멀티 클라우드 방어 컨트롤러 쉬운 설정 모달에서 생성된 명령을 복사하여 클라우드 쉘에 붙여넣습니다. 명령을 실행하여 온보딩 프로세스를 시작합니다. 이 스크립트는 멀티 클라우드 방어 컨트롤러이(가) GCP 프로젝트와 직접 통신할 수 있도록 사용자 계정을 자동으로 생성합니다.

c) 멀티 클라우드 방어 컨트롤러 쉬운 설정 모달에서 계정의 이름을 입력합니다. GCP 프로젝트 이름과 동일하게 이름을 지정할 수 있습니다. 이 이름은 멀티 클라우드 방어 컨트롤러에서만 표시됩니다.

d) (선택 사항) **Description(**설명**)**을 입력합니다.

e) GCP 프로젝트의 프로젝트 **ID**를 입력합니다.

f) 멀티 클라우드 방어 컨트롤러에 대해 생성된 서비스 어카운트의 **Client Email(**클라이언트 이메일**)**을 입력합니다.

g) 서비스 어카운트의 개인 키를 입력합니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

OCI 연결

OCI(Oracle Cloud) 계정을 온보딩하기 전에 다음 사전 요건을 실행해야 합니다.

OCI에 로그인

1. OCI 테넌트에 로그인합니다.

그룹 생성

단계 **1** **Identity & Security(ID** 및 보안**)** > **Groups(**그룹**)**로 이동합니다.
단계 **2** **Create Group(**그룹 생성**)**을 클릭합니다.
단계 **3** 다음 항목을 지정합니다.

- **Name(**이름**):** 멀티 클라우드 방어-controller-group
- **Description(**설명**):** 멀티 클라우드 방어 그룹

단계 **4** **Create(**생성**)**를 클릭합니다.

정책 생성

멀티 클라우드 방어로 OCI 어카운트를 생성하는 경우 방화벽 정책을 생성하고 적용해야 합니다. 다음 절차와 권장 사항에 따라 정책을 생성합니다.

단계 **1** **Identity & Security(ID** 및 보안**)** > **Policies(**정책**)**로 이동합니다.
단계 **2** **Compartment(**컴파트먼트**)** *root(*루트*)*를 선택합니다.
단계 **3** **Create Policy(**정책 생성**)**를 클릭합니다.
단계 **4** 다음 항목을 지정합니다.

- **Name(**이름**):** 멀티 클라우드 방어-controller-policy.
- **Description(**설명**):** 멀티 클라우드 방어 정책.
- **Compartment(**컴파트먼트**):** ["root" 컴파트먼트여야 함].

단계 **5** **Policy Builder(**정책 빌더**)**에서 **Show manual Editor(**수동 편집기 표시**)**를 활성화합니다.
단계 **6** 다음 정책 수정 및 붙여넣기

```
Allow group <group_name> to inspect instance-images in compartment <compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to use volume-family in compartment <compartment_name>
Allow group <group_name> to use virtual-network-family in compartment <compartment_name>
Allow group <group_name> to manage volume-attachments in compartment <compartment_name>
Allow group <group_name> to manage instances in compartment <compartment_name>
```

```
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment <compartment_name>
Allow group <group_name> to manage load-balancers in compartment <compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to manage app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to read virtual-network-family in tenancy
Allow group <group_name> to read instance-family in tenancy
Allow group <group_name> to read load-balancers in tenancy
```

- **group_name:** 멀티 클라우드 방어-controller-group.
- **compartment_name:**[멀티 클라우드 방어이(가) 구축될 컴파트먼트].

Note Cisco IOS 시스템을 교체할 때 **<compartment_name>**을 정책을 적용할 구역의 이름으로 바꿉니다. 구역이 하위 구역인 경우, 이름 형식은 **compliance:sub-compartment**(예: Prod:App1)입니다.

<compartment_name>이 루트 컴파트먼트(예: multicloud (root))로 지정된 경우 OCI는 정책을 수락하지 않고 오류: *Invalid parameter(*잘못된 매개변수*)*가 생성됩니다. 특정 컴파트먼트에 대해 정책을 정의해야 하며 해당 컴파트먼트는 루트 컴파트먼트일 수 없습니다.

단계 **7** **Create(**생성**)**를 클릭합니다.

사용자 생성

단계 **1** **Identity & Security(ID** 및 보안**)** > **Users(**사용자**)**로 이동합니다.
단계 **2** **Create User**(사용자 생성)를 클릭합니다.
단계 **3** 다음 항목을 지정합니다.

- **Name(**이름**):** 멀티 클라우드 방어*-controller-user*
- **Description(**설명**):** 멀티 클라우드 방어 *User(*사용자*)*

단계 **4** **Create(**생성**)**를 클릭합니다.

API 키 생성

단계 **1** 사용자에 대한 **User Details(**사용자 세부 정보**)** 보기에서 **API Keys(API** 키**)**를 선택합니다.
단계 **2** **Add API Key(API** 키 추가**)**를 클릭합니다.
단계 **3** **Download Private Key(**개인 키 다운로드**)**를 선택하고 나중에 사용할 수 있도록 개인 키를 보관합니다.
단계 **4** **Download Public Key(**공개 키 다운로드**)**를 선택하고 나중에 사용할 수 있도록 공개 키를 보관합니다.
단계 **5** **Add(**추가**)**를 클릭합니다.

약관 동의

다음 절차에 따라 OCI 어카운트의 이용 약관에 동의합니다.

단계 **1** **Compute**(계산) > **Instance**(인스턴스)를 선택합니다.
단계 **2** 원하는 **Compartment**(컴파트먼트)를 선택합니다.
단계 **3** **Create instance**(인스턴스 생성)를 클릭합니다.
단계 **4** **Image and shape**(이미지 및 모양)에서 **Change image**(이미지 변경)를 선택합니다.
단계 **5** **Image source**(이미지 소스)에서 **Community Images**(커뮤니티 이미지)를 선택합니다.
단계 **6** 멀티 클라우드 방어 검색을 수행합니다.
단계 **7** 멀티 클라우드 방어에 대한 확인란을 선택합니다.
단계 **8** *I have reviewed and accept the Publishers terms of use, Oracle Terms of Use, and the Oracle General Privacy Policy*(본인은 게시자 이용 약관, 오라클 이용 약관 및 오라클 일반 개인정보 취급방침을 검토하고 이에 동의합니다.)에 대한 상자를 선택합니다.
단계 **9** **Select Image**(이미지 선택)를 클릭합니다.
단계 **10** 종료합니다(이미지를 구축하지 않음).

멀티 클라우드 방어 게이트웨이을(를) 구축하려는 각 컴파트먼트에 대해 단계를 반복합니다.

Oracle 어카운트 연결

다음 절차에 따라 멀티 클라우드 방어 컨트롤러의 쉬운 설정 마법사를 통해 OCI 어카운트에 연결합니다.

시작하기 전에

- 기존 OCI(Oracle Cloud) 계정이 있어야 합니다.
- 온보딩 전에 OCI 계정에 대한 사전 요구 사항을 완료해야 합니다. 자세한 내용은 OCI 연결, 5 페이지를 참조하십시오.
- CDO 테넌트가 있어야 합니다.
- CDO 테넌트에 관리자 또는 슈퍼 관리자 사용자 역할이 있어야 합니다.
- CDO 테넌트에 대해 멀티 클라우드 방어을(를) 활성화해야 합니다.

단계 **1** CDO 대시보드에서 왼쪽 탐색 창에 있는 멀티 클라우드 방어 탭을 클릭합니다.
단계 **2** 오른쪽 상단 창에 있는 멀티 클라우드 방어 컨트롤러을 클릭합니다.
단계 **3** 멀티 클라우드 방어 컨트롤러 대시보드에서 창 왼쪽에 있는 **Setup**(설정)을 클릭합니다.
단계 **4** **Connect Account**(어카운트 연결)를 선택합니다.
단계 **5** OCI 아이콘을 선택합니다.

단계 **6** 모달에 다음 정보를 입력합니다.

a) **OCI Account Name(OCI** 계정 이름**)**을 입력합니다. 이 이름은 멀티 클라우드 방어 컨트롤러에서만 사용되며 식별 목적으로만 사용됩니다.
b) (선택 사항) 계정 설명을 입력합니다.
c) **Tenancy OCID(**테넌시 **OCID)**를 입력합니다. 이는 OCI 사용자로부터 가져온 테넌시 Oracle Cloud 식별자입니다.
d) OCI 사용자에게 할당된 개인 키를 입력합니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

계정을 연결하면 멀티 클라우드 방어 컨트롤러이(가) 클라우드 서비스 제공자 계정과 연결된 자산 및 인벤토리 목록을 검색하기 시작합니다. 이는 트래픽 검색과는 다릅니다. 멀티 클라우드 방어 컨트롤러은(는) 기본적으로 계정 자산 및 인벤토리 목록을 검색하므로 이 마법사의 다음 단계는 트래픽 가시성 활성화하는 것입니다.

트래픽 가시성 활성화

트래픽 가시성을 활성화하면 다음 로그를 수집하여 클라우드 어카운트 내의 트래픽 플로우를 확인할 수 있습니다.

- NSG 플로우 로그
- (**AWS**만 해당) VPC 플로우 로그
- DNS 로그
- Route53 쿼리 로깅

흐름 및 DNS 쿼리 로그는 멀티 클라우드 방어에서는 트래픽 흐름을 파악하고, 위협 인텔리전스 피드와 상호 연결하고, 멀티 클라우드 방어을(를) 사용하여 보호할 수 있는 기존 위협에 대한 통찰력을 제공하는 데 사용됩니다.

트래픽 가시성을 활성화하는 것은 클라우드 어카운트 유형마다 다른 프로세스이지만, 일반적으로 클라우드 어카운트의 지역, 모니터링할 VPC/VNet, 네트워크 보안 그룹 및 로그용 클라우드 스토리지 어카운트과 같은 어카운트 특성을 식별해야 합니다.

설정 마법사에서 트래픽 가시성을 활성화하려면 다음 절차를 사용합니다.

시작하기 전에

이미 하나 이상의 클라우드 서비스 제공자 계정을 멀티 클라우드 방어 컨트롤러에 연결해야 합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 포털의 왼쪽 내비게이션 바에서 **Setup(**설정**)**을 클릭합니다.

단계 **2** 설정 마법사에서 **Enable Traffic Visibility(**트래픽 가시성 활성화**)**를 클릭합니다.

단계 **3** **CSP Account(CSP** 계정**)** - 드롭다운 메뉴를 사용하여 멀티 클라우드 방어 컨트롤러이(가) 서비스 VPC/VNet을 구축할 클라우드 서비스 제공자 계정을 선택합니다.

단계 **4** **Region(**지역**)** - 드롭다운 메뉴를 사용하여 선택한 클라우드 서비스 제공자가 위치한 지역을 선택합니다.

단계 **5** 선택한 클라우드 서비스 제공자 유형에 적용 가능한 사용 가능한 VPC 테이블을 스크롤하여 적절한 VPC를 선택합니다. VPC가 즉시 표시되지 않는 경우 **Refresh(**새로 고침**)** 아이콘을 클릭하여 현재 목록을 새로 고칩니다.

단계 **6** (선택 사항) 드롭다운 메뉴를 사용하여 계정에서 DNS 쿼리 및 VPC 흐름 로그가 저장되는 S3 버킷을 선택합니다. 선택한 S3 버킷은 트래픽을 활성화할 때 프로세스의 일부로 멀티 클라우드 방어에 의해 생성됩니다.

단계 **7** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

어카운트를 보호합니다.

어카운트 보안

중앙 집중식 또는 분산형 모델에 구축된 게이트웨이로 계정을 보호합니다.

중앙 집중식 모델에서는 멀티 클라우드 방어가 게이트웨이를 포함하기 위해 VPC 또는 VNet을 오케스트레이션하고 구축합니다. 즉, VPC 또는 VNet 및 필요한 모든 추가 구성 요소는 이 구문 내에서 게이트웨이의 구축과 함께 오케스트레이션됩니다.

분산형 모델에서 멀티 클라우드 방어는 네트워크에서 이미 사용 가능한 기존 인프라 내에서 게이트웨이를 빌드하고 구축합니다.

어카운트를 보호하려면 아래 절차 중 하나를 계속 진행합니다.

중앙 집중식 모델: **VPC** 또는 **VNet** 추가

다음 절차에 따라 게이트웨이를 수용하고 계정을 보호할 VPC 또는 VNet을 만들고 추가합니다.

시작하기 전에

이 마법사를 시작하기 전에 하나 이상의 클라우드 서비스 제공자가 멀티 클라우드 방어 컨트롤러에 연결되어 있어야 합니다. 일부 사업자의 경우, 이 절차는 필수 매개변수에 따라 변경됩니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 포털의 왼쪽 내비게이션 바에서 **Setup(**설정**)**을 클릭합니다.

단계 **2** 설정 마법사에서 **Secure Account(**어카운트 보안**)**를 클릭합니다.

단계 **3** **Centralized(**중앙 집중식**)**를 선택하면 강조 표시됩니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** 서비스 VPC/VNet 추가:

a) **Name(**이름**)** - 서비스 VPC/VNet의 이름을 입력합니다. 생성되면 이 이름이 **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Service VPC/VNETS(**서비스 **VPC/VNETS)** 페이지에 표시됩니다.

b) **CSP Account(CSP** 계정**)** - 드롭다운 메뉴를 사용하여 멀티 클라우드 방어 컨트롤러에 이미 연결된 클라우드 서비스 제공자 계정을 선택합니다. 서비스 VPC/VNet이 선택한 계정에 구축됩니다.
c) **Region(**지역**)** - 드롭다운 메뉴를 사용하여 선택한 클라우드 서비스 제공자가 있는 지역을 선택합니다.
d) **CIDR Block(CIDR** 차단**)** - 서비스 VPC/VNet이 연결되는 Transit Gateway의 고유한 값을 입력합니다.
e) **Availablity Zones(**가용성 영역**)** - 생성된 목록에서 가용성 영역을 하나 이상 선택합니다. 최상의 결과를 얻으려면 영역 2개를 선택하는 것이 좋습니다.
f) (Azure 계정만 해당) **Resource Group(**리소스 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이를 연결할 리소스 그룹을 선택합니다. 현재 나열되지 않은 경우 이 화면에서 **Create Resource Group(**리소스 그룹 생성**)**을 수행할 수 있습니다.
g) (AWS 계정만 해당) **Transit Gateway(Transit Gateway)** - 드롭다운 메뉴를 사용하여 VPC에 연결할 사용 가능한 Transit Gateway를 선택합니다. 없는 경우 **create_new**를 클릭하여 이 창에서 Transit Gateway를 생성합니다.
h) (AWS 어카운트에만 해당) **Use NAT Gateway(NAT** 게이트웨이 사용**)** - 모든 이그레스 트래픽이 NAT 게이트웨이를 통과하도록 하려면 이 옵션을 선택합니다. 멀티 클라우드 방어에서는 선택된 각 가용성 영역에 대해 NAT 게이트웨이를 자동으로 생성합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

게이트웨이를 추가합니다.

분산형 모델

분산형 게이트웨이 모델의 경우 사용 중인 클라우드 서비스 제공자에 따라 다음 절차를 사용합니다.

Azure 분산형 모델**:** 게이트웨이 생성

다음 절차를 사용하여 분산형 모델로 Azure 계정용 게이트웨이를 생성합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 포털의 왼쪽 내비게이션 바에서 **Setup(**설정**)**을 클릭합니다.
단계 **2** 설정 마법사에서 **Secure Account(**어카운트 보안**)**를 클릭합니다.
단계 **3** **Distributed(**분산됨**)**를 선택하면 강조 표시됩니다.
단계 **4** **Next(**다음**)**를 클릭합니다.
단계 **5** 다음 게이트웨이 정보를 입력합니다.
a) **Account(**계정**)** - 드롭다운 메뉴를 사용하여 게이트웨이를 구축할 Azure 계정을 선택합니다.
b) **Name(**이름**)** - 게이트웨이 이름을 입력합니다. 이 이름은 **Manage(**관리**)** > **Gateways(**게이트웨이**)** 페이지에 표시됩니다.
c) (선택 사항) **Description(**설명**)** - 다른 게이트웨이와 구별하는 게이트웨이의 설명을 입력합니다.
d) **Instance Type(**인스턴스 유형**)** - 드롭다운 메뉴를 사용하여 게이트웨이를 구축하는 인스턴스 유형을 선택합니다.
e) **Minimum Instances(**최소 인스턴스**)** - 가용성 영역당 자동 확장 그룹에 구축되는 최소 인스턴스 수를 선택합니다.

f) **Maximum Instance(**최대 인스턴스**)** - 가용성 영역당 자동 확장 그룹에 구축되는 최대 인스턴스 수를 선택합니다.

g) **HealthCheck Port(**상태 확인 포트**)** - 상태 확인 포트 번호를 입력합니다. 멀티 클라우드 방어 컨트롤러에서는 기본값으로 `65534`를 사용합니다.

h) **User Name(**사용자 이름**)** - 생성된 게이트웨이에 액세스하는 데 사용되는 사용자 이름을 입력합니다.

i) **Packet Capture Profile(**패킷 캡처 프로파일**)** - 드롭다운 메뉴를 사용하여 클라우드 스토리지 버킷에서 패킷이 저장되는 위치를 선택합니다. 옵션이 나열되지 않는 경우 **Create Packet Capture Profile(**패킷 캡처 프로파일 생성**)**을 클릭하여 이 창에서 하나를 생성합니다.

j) **Log Profile(**로그 프로파일**)** - 드롭다운 메뉴를 사용하여 어떤 클라우드 서비스 제공자에 로깅을 전달할지 선택합니다.

k) **Metrics Profile(**메트릭 프로파일**)** - 드롭다운 메뉴를 사용하여 메트릭을 전달할 엔터티를 선택합니다. 옵션이 나열되지 않는 경우 **Create Metrics Forward Profile(**메트릭 전달 프로파일 생성**)**을 클릭하여 이 창에서 생성합니다.

l) **NTP Profile(NTP** 프로파일**)** - 드롭다운 메뉴를 사용하여 게이트웨이와 연결된 NTP 프로파일을 선택합니다. 옵션이 나열되지 않으면 **Create(**생성**)**를 클릭하여 이 창에서 옵션을 생성합니다.

m) **Security(**보안**)** - 게이트웨이가 처리해야 하는 트래픽 플로우의 유형을 선택합니다. 인그레스 보안은 공용 인터넷에서 프라이빗 네트워크로 이동하는 트래픽을 대상으로 합니다. 이스트-웨스트 및 이그레스 보안은 프라이빗 네트워크에서 아웃바운드하는 트래픽과 데이터 센터 간에 이동하는 트래픽을 대상으로 합니다.

n) **Gateway Image(**게이트웨이 이미지**)** - 드롭다운 메뉴를 사용하여 게이트웨이에 구축할 게이트웨이 이미지를 선택합니다.

o) **Policy Ruleset(**정책 규칙 집합**)** - 드롭다운 메뉴를 사용하여 구축할 정책 규칙 집합을 선택하고 트래픽 처리를 시작합니다. 규칙 집합이 목록에 없으면 **Create new(**새로 만들기**)**를 클릭하여 이 창에서 정책 규칙 집합을 생성합니다.

p) **Region(**지역**)** - 드롭다운 메뉴를 사용하여 게이트웨이가 구축된 지역을 선택합니다.

q) **VPC/VNet ID** - 드롭다운 메뉴를 사용하여 게이트웨이가 구축된 VPC를 선택합니다.

r) **Key Selection(**키 선택**)** - SSH 공개 키 또는 SSH 키 쌍을 선택합니다. 게이트웨이에 적용할 값을 다음 텍스트 필드에 입력합니다.

s) **Resource Group(**리소스 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이에 적용되는 기존 리소스 그룹을 선택합니다.

t) **User Assigned Identity ID(**사용자 할당 **ID)** - 유효한 값을 입력합니다.

u) **Mgmt. Security Group(**관리 보안 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이 관리 인터페이스에 사용되는 보안 그룹을 선택합니다. 멀티 클라우드 방어에서 생성된 서비스 VPC를 선택할 경우 관리용으로 보안 그룹이 특별히 생성됩니다.

v) **Datapath Security Group(**데이터 경로 보안 그룹**)** - 드롭다운 메뉴를 사용하여 게이트웨이 데이터 경로 인터페이스에 사용되는 보안 그룹을 선택합니다. 멀티 클라우드 방어에서 생성한 서비스 VPC를 선택할 경우 해당 데이터 경로에 특별히 보안 그룹이 생성됩니다.

w) **Disk Encryption(**디스크 암호화**)** - Azure 관리 암호화 또는 고객 관리 암호화 키를 사용하여 디스크 암호화를 활성화합니다. 고객 관리 암호화 키를 선택하는 경우 성공적인 구축을 위해 IAM 정책을 생성하고 구축해야 합니다.

x) **Availability Zone(**가용성 영역**)** - 드롭다운 메뉴를 사용하여 가용성 영역을 선택합니다.

y) **Mgmt. Subnet(**관리 서브넷**)** - 드롭다운 메뉴를 사용하여 관리 인터페이스의 관리 서브넷을 선택합니다.

z) **Datapth Subnet(**데이터 경로 서브넷**)** - 드롭다운 메뉴를 사용하여 데이터 경로 인터페이스의 서브넷을 선택합니다.

인스턴스 유형을 더 추가하려면 "+" 아이콘을 클릭합니다. 이어서 "-" 아이콘을 사용하여 추가 인스턴스 유형을 제거할 수 있습니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 다음 고급 설정을 입력합니다.

a)

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** 검토

다음에 수행할 작업