멀티 클라우드 방어 게이트웨이 관리

개요

멀티 클라우드 방어 게이트웨이은(는) 멀티 클라우드 방어 게이트웨이 인스턴스의 클러스터가 있는 네트워크 로드 밸런서로 구성된 네트워크 기반 보안 플랫폼입니다. 이 클러스터는 트래픽 로드에 따라 확장 및 축소되는 자동 확장 및 자가 복구 클러스터입니다. 멀티 클라우드 방어 컨트롤러 및 게이트웨이 인스턴스는 상태 및 텔레메트리에 관한 일정하고 지속적인 정보를 교환합니다. 멀티 클라우드 방어 컨트롤러은(는) 게이트웨이 인스턴스에서 수신된 텔레메트리 데이터를 측정하여 확장/축소 결정을 내립니다. 고 가용성의 탄력적 아키텍처를 위해 여러 가용성 영역에서 게이트웨이를 실행하도록 구성할 수 있습니다. 이렇게 하면 클라우드 서비스 공급자의 단일 가용성 영역 장애가 발생해도 실행 중인 애플리케이션의 보안 상태가 손상되지 않습니다.

게이트웨이 및 해당 VPC 또는 VNet을 구성한 후에는 멀티 클라우드 방어 컨트롤러의 **Gateway Details(**게이트웨이 세부 정보**)** 페이지를 사용하여 해당 상태를 보고 관리할 수 있습니다.

멀티 클라우드 방어 게이트웨이는 두 가지 방법으로 구축할 수 있습니다. 허브 모드와 엣지 모드입니다.

게이트웨이 재시도

멀티 클라우드 방어 게이트웨이는 자가 복구 구성 요소 멀티 클라우드 방어입니다. 어느 시점에서든 게이트웨이 구축이 실패하거나 문제가 발생하면, 멀티 클라우드 방어는 자동으로 게이트웨이 재시도를 포함한 게이트웨이 재구축을 시도합니다. 이 작업은 컨트롤러에서 게이트웨이를 수동으로 비활성화하거나 삭제할 때까지 무제한으로 수행됩니다.

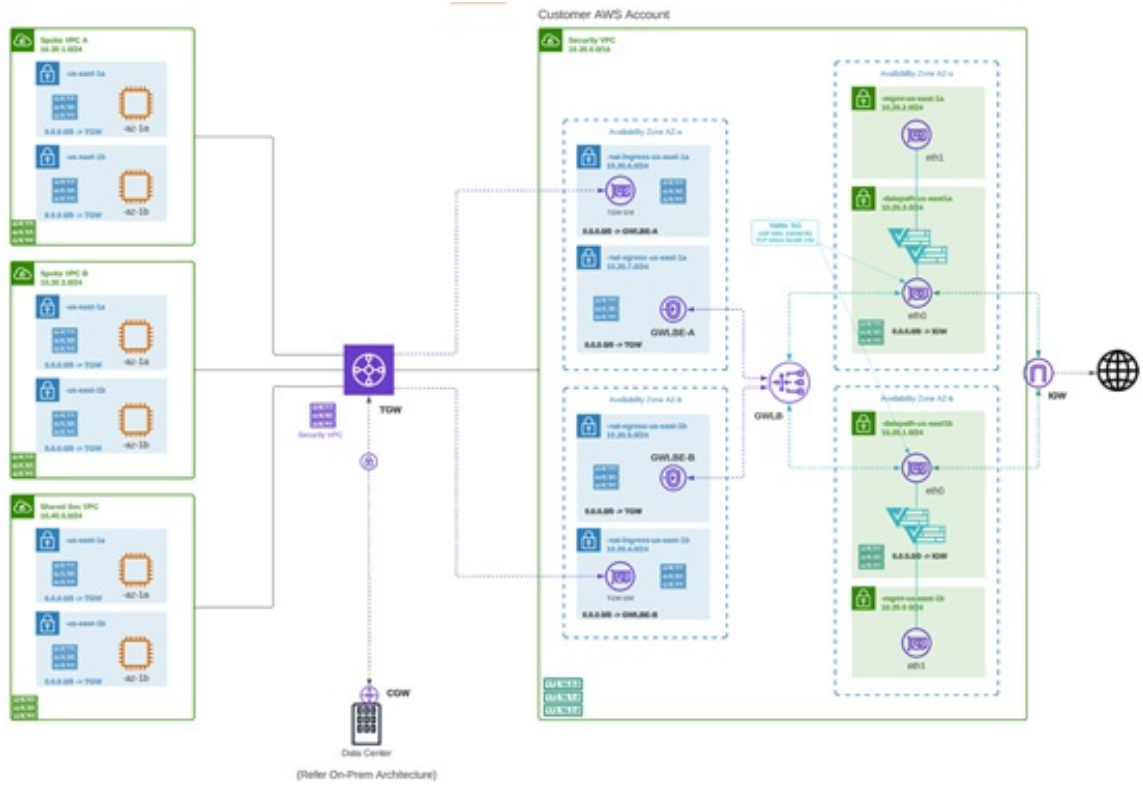
Terraform에서 두 가지 측면의 재시도 작업을 설정할 수 있습니다. 첫 번째, 게이트웨이 구축을 위해 멀티 클라우드 방어가 재시도하는 횟수를 구성할 수 있습니다. 최대 재구축 시도 횟수가 완료되면 멀티 클라우드 방어은 재시도를 중지합니다. 둘째, 재시도 사이의 시간을 구성할 수 있습니다. 예를 들어, 게이트웨이 재시도를 한 시간에 3회 구성할 수 있습니다. 즉, 1시간마다 멀티 클라우드 방어가 게이트웨이 구축을 3회 재시도한 다음 중지됩니다. 이 작업은 게이트웨이 문제가 해결되거나 컨트롤러에서 게이트웨이를 삭제하는 경우까지 반복됩니다.

지원되는 게이트웨이 활용 사례

이그레스

퍼블릭 클라우드 네트워크에서 나가는 트래픽을 보호하기 위해 이그레스/이스트-웨스트 게이트웨이 구축. 이그레스 게이트웨이는 투명 전달 프록시로 작동하여 전체 암호 해독을 수행하고 침입 방지, 악성코드 차단, 데이터 손실 방지, 전체 경로 URL 필터링과 같은 고급 보안 기능을 내장합니다. 선택적으로, 전달 모드에서 작동할 수도 있습니다. 이 모드에서는 트래픽을 프록시하거나 암호 해독하지 않지만 악의적인 IP 차단 및 FQDN 필터링과 같은 보안 기능이 계속 적용됩니다.

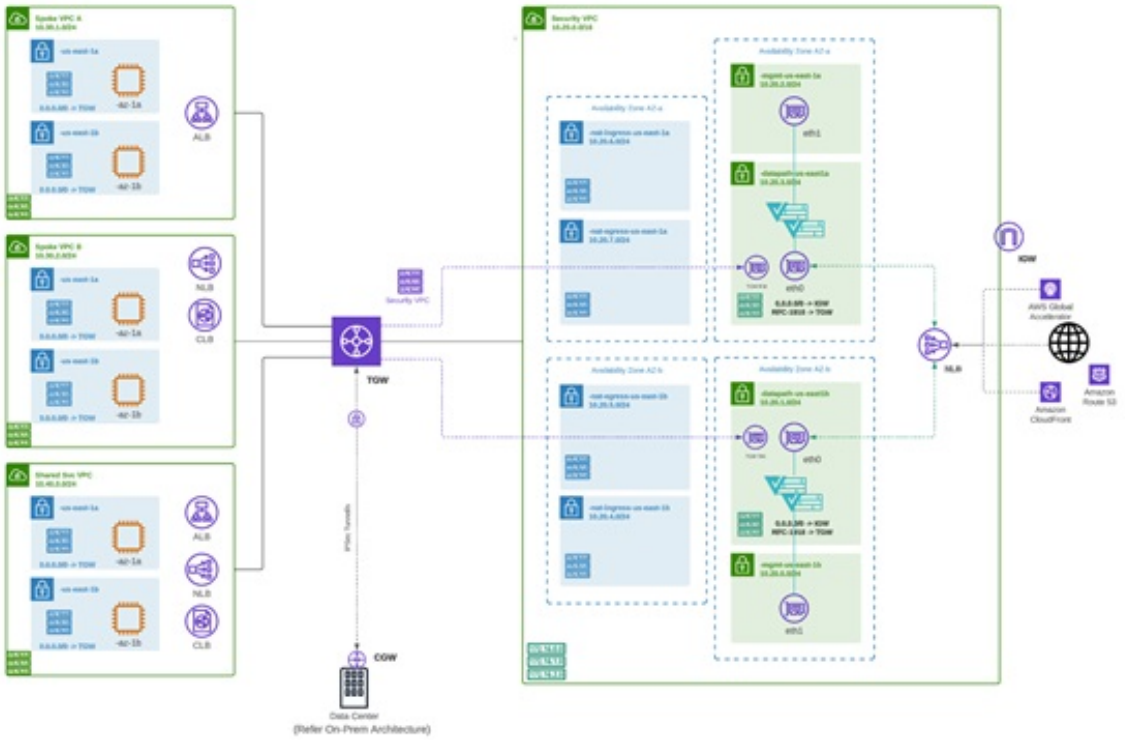
다음 다이어그램은 중앙 집중식 모드의 이그레스 게이트웨이가 있는 AWS 계정의 예입니다.



인그레스

인그레스 게이트웨이를 구축하면 공용으로 연결되는 애플리케이션이 보호됩니다. 인그레스 게이트웨이는 전체 암호 해독을 수행하고 침입 방지, 악성코드 차단, WAF(Web Application Firewall), 전체 경로 URL 필터링과 같은 고급 보안 기능을 적용하는 역방향 프록시 역할을 합니다.

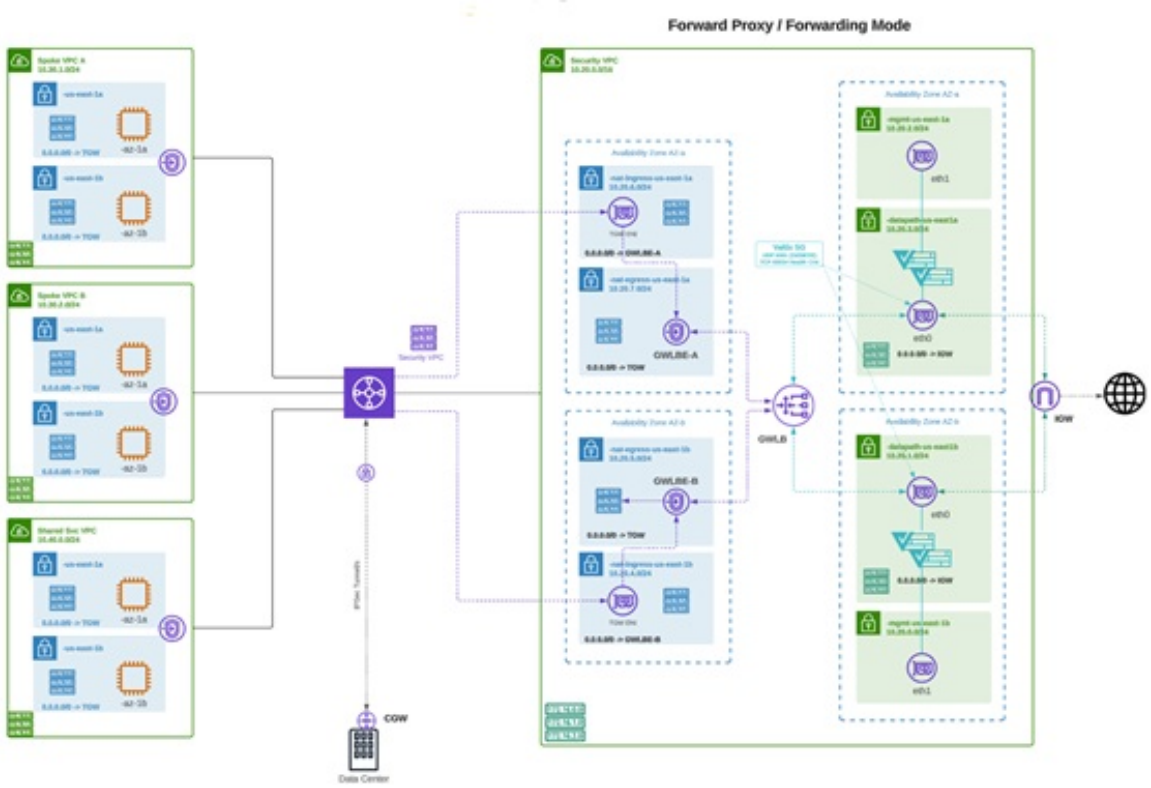
다음 다이어그램은 중앙 집중식 모드의 인그레스 게이트웨이가 있는 AWS 계정의 예입니다.



East-West

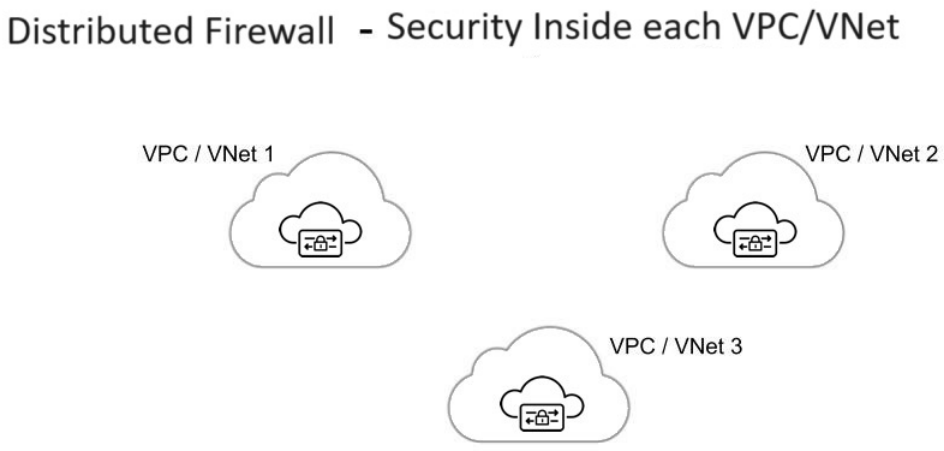
이그레스/이스트-웨스트 게이트웨이 구축은 퍼블릭 클라우드 환경 내에서 서브넷 또는 VPC/Vnet 간에 이스트-웨스트 L4 세분화를 구현합니다. 게이트웨이는 L4 방화벽 규칙을 통해 전달 모드로 작동하여 선택적 로깅이 활성화된 상태에서 설정된 매개변수를 기반으로 트래픽을 허용하거나 거부합니다.

다음 다이어그램은 중앙 집중식 모드의 이스트-웨스트 게이트웨이가 있는 AWS 계정의 예입니다.



분산화

여러 VPC/VNet에서 애플리케이션을 실행 중입니다. 각 VPC/VNet에 멀티 클라우드 방어 게이트웨이을(를) 구축합니다.



중앙 집중식/허브

여러 VPC/VNet에서 애플리케이션을 실행 중입니다. 중앙 집중식 보안 서비스 VPC/VNet을 통해 모든 애플리케이션을 보호하려고 합니다. 이 모델은 서비스 VPC에 멀티 클라우드 방어 게이트웨이를 구축합니다. 모든 애플리케이션 VPC(스포크 VPC)와 서비스 VPC를 Azure 및 GCP의 AWS Transit Gateway 또는 VNet/VPC 피어링에 연결합니다. 멀티 클라우드 방어는 AWS Transit Gateway, 서비스 VPC 및 스포크 VPC 첨부 파일을 오케스트레이션하는 옵션을 제공합니다. 이 솔루션은 여러 경로 테이블 및 Transit Gateway 첨부 파일의 복잡성을 제거하여 손쉽게 구축할 수 있는 권장 솔루션입니다.

Figure 1: AWS - AWS Transit Gateway 사용

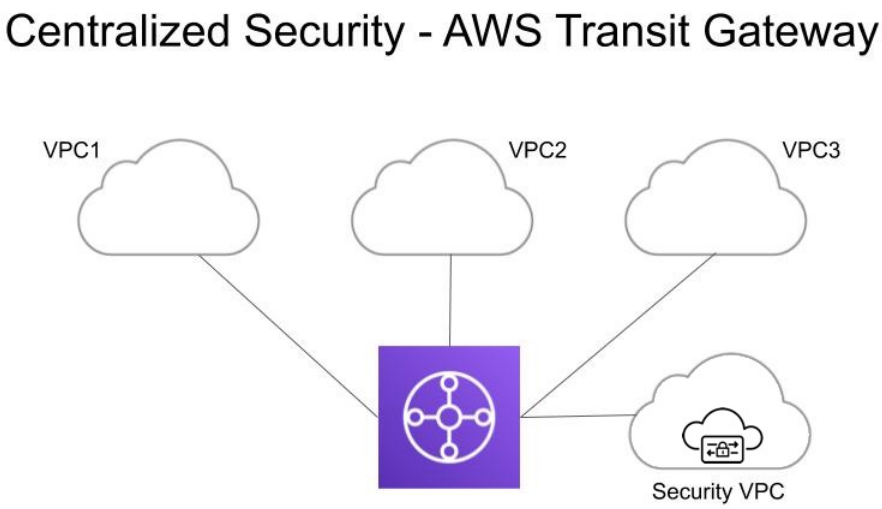


Figure 2: Azure - VNet 피어링

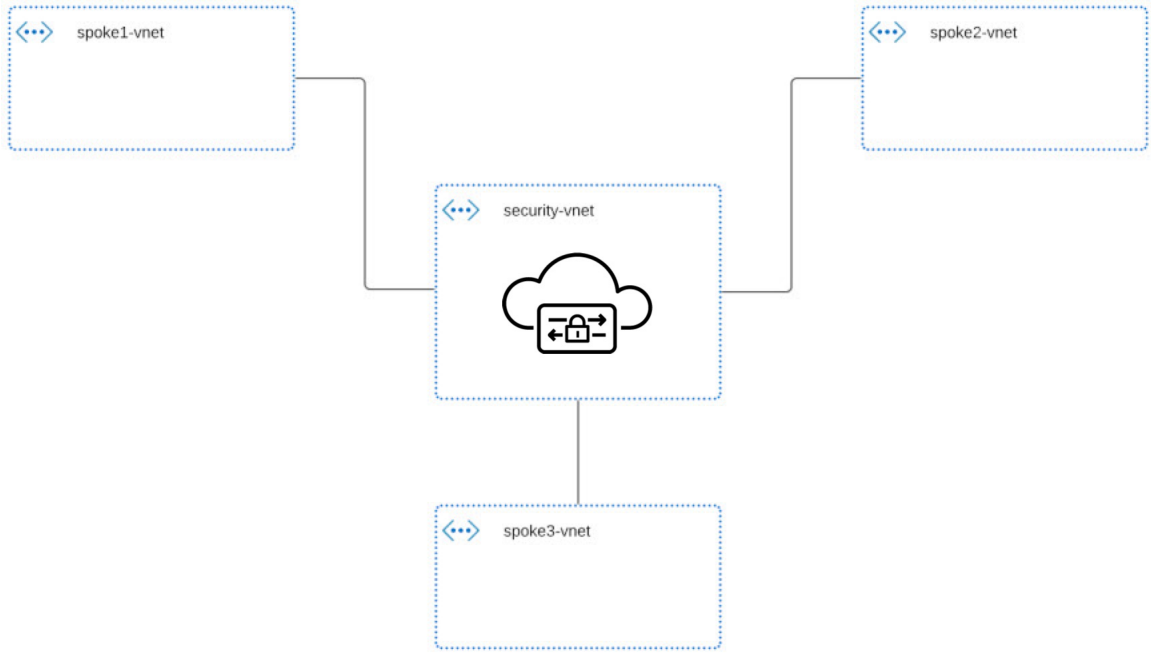
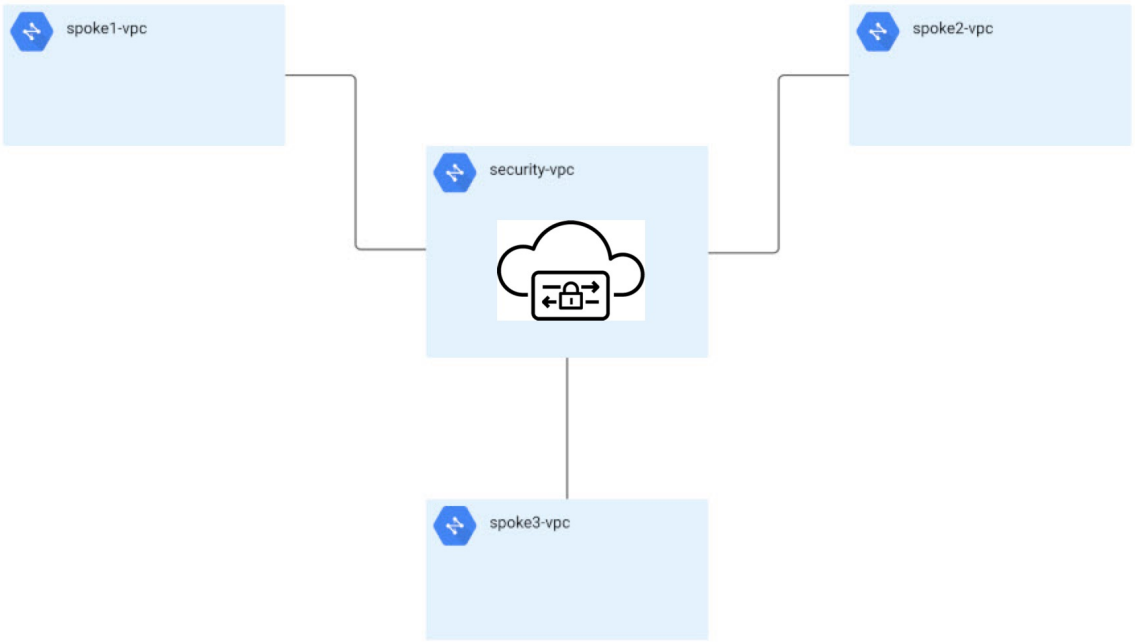


Figure 3: GCP - VPC 피어링



고급 활용 사례

일부 게이트웨이의 경우 추가 사전 요건 또는 사후 절차 단계가 있을 수 있습니다. 다음 환경을 고려하십시오.

AWS: 인그레스 게이트웨이에 대한 가속기

멀티 클라우드 방어는 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 멀티 클라우드 방어 인그레스 게이트웨이로 전역 가속기를 통과할 때 유지됩니다.

멀티 클라우드 방어를 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.

게이트웨이 세부 정보

이미 설정된 게이트웨이에 대한 **Gateway Details(**게이트웨이 세부 정보**)** 페이지를 보는 방법은 **Manage(**관리**)** > **Gateways(**게이트웨이**)**에서 이미 설정한 게이트웨이를 사용할 수 있습니다. 이 페이지에서 모든 게이트웨이를 추가하고 관리할 수 있습니다. 게이트웨이를 관리하면 인스턴스를 편집, 업그레이드, 활성화, 비활성화, 내보내기 또는 삭제할 수 있습니다. 변경하기 전에 수정할 게이트웨이의 확인란을 클릭해야 합니다.

참고 이러한 작업을 수행하려면 관리자 또는 슈퍼 관리자여야 합니다.

다음 기준을 사용하여 게이트웨이 목록을 필터링하고 검색하려면 다음 항목 중 하나를 사용할 수 있습니다.

- **Name(**이름**)** - 게이트웨이의 이름입니다.
- **CSP Account(CSP** 계정**)** - 게이트웨이와 연결된 클라우드 서비스 제공자 계정입니다.
- **CSP Type(CSP** 유형**)** - 클라우드 서비스 제공자 계정의 유형입니다.
- **Region(**지역**)** - 검색 중인 게이트웨이와 연결된 클라우드 서비스 제공자의 지역입니다.
- **State(**상태**)** - 게이트웨이의 현재 상태입니다. 게이트웨이는 활성 또는 비활성, 또는 보류 중인 활성 또는 보류 중인 비활성 상태일 수 있습니다.
- **Instance Type(**인스턴스 유형**)** - 각 클라우드 서비스 제공자는 여러 인스턴스 유형을 지원합니다.
- **Mode(**모드**)** - 허브 또는 엣지 모드에서 멀티 클라우드 방어 게이트웨이 인스턴스를 구축할 수 있습니다.

Switch to Advanced Search(고급 검색으로 전환**)**를 클릭하여 검색을 직접 구성합니다. 필요한 경우 검색 창의 드롭다운 옵션을 사용하여 자동 생성된 검색 기준을 활용합니다. 를 반복해야 하는 검색의 경우 나중에 사용할 수 있도록 검색을 복사하거나 저장할 수 있습니다.

멀티 클라우드 방어 게이트웨이 및 **VPC/VNet** 구성

시작하기 전에

지원되는 클라우드 서비스 제공자는 고유한 용어 및 게이트웨이 환경을 사용하는 별도의 엔터티입니다. 멀티 클라우드 방어 컨트롤러에서 사용 가능한 모든 옵션이 클라우드 서비스 제공자와 호환되는 것은 아닙니다. 예를 들어 AWS는 자체 Transit 게이트웨이를 사용하며 사용자는 VPC를 추가할 수 있으며 Azure에서는 로드 밸런서를 사용하여 웹 트래픽 및 애플리케이션을 관리하며 사용자는 여기에 VNet을 추가할 수 있습니다. 계속 진행할 때 이 점에 유의하십시오.

참고 AWS 환경의 경우 중앙 집중식 모드에서 스포크 VPC를 보호할 때 멀티 클라우드 방어은 VPC를 서비스 VPC와 연결된 Transit Gateway에 연결합니다. 기본적으로 멀티 클라우드 방어은(는) Transit Gateway 연결에 대해 각 가용성 영역에서 서브넷을 무작위로 선택합니다. VPC를 추가할 때 이 옵션을 변경할 수도 있고, 게이트웨이에 이미 할당된 VPC를 수정할 수도 있습니다.

멀티 클라우드 방어 게이트웨이를 통해 Transit Gateway를 오케스트레이션하거나 기존 Transit Gateway를 연결할 수도 있습니다.

제한 사항

멀티 클라우드 방어 게이트웨이를 생성할 때 다음 제한 사항에 유의합니다.

- IPSec 프로파일이 포함된 사이트 간 VPN 터널을 사용하는 멀티 클라우드 방어 게이트웨이을 구축하는 경우, VPN 연결의 양쪽에 NAT(Network Address Translation) 게이트웨이 없이 서비스 VPC 또는 서비스 VNet을 사용하여 게이트웨이를 구축해야 합니다.
- IPSec 프로파일을 포함하는 게이트웨이에 대해서는 Autoscaling이 지원되지 않습니다.
- 게이트웨이 내의 정책 규칙은 전달 전용이어야 합니다.
- AWS 또는 Azure 어카운트에 대한 멀티 클라우드 방어 게이트웨이에 IPSec 프로파일을 포함하려면 코어 8 로 게이트웨이 인스턴스를 설정 해야 합니다. 멀티 클라우드 방어 게이트웨이는 현재 코어 2 또는 코어 4 옵션이 있는 게이트웨이를 지원하지 않습니다.

멀티 클라우드 방어에서 생성한 리소스

다음 리소스는 게이트웨이, VPC 또는 VNet을 생성할 때 멀티 클라우드 방어에 의해 생성됩니다. 이러한 프로세스의 일부로 생성되며 사용자의 추가 작업이 필요하지 않습니다. 각 클라우드 서비스 제공자 요구 사항에 따라 다른 리소스가 생성됩니다.

GCP 리소스

멀티 클라우드 방어은(는) 2개의 서비스 VPC와 4개의 방화벽을 생성합니다. 정확한 리소스 할당은 다음을 참조하십시오.

Service VPC(서비스 **VPC)**

- 관리
- 데이터 경로

방화벽 규칙

- 관리(인그레스)
- 관리(이그레스)
- 데이터 경로(이그레스)
- 데이터 경로(이그레스)

참고 서비스 VPC CIDR은 스포크 VPC와 중복될 수 없습니다.

AWS 리소스

멀티 클라우드 방어은(는) 지원되는 활용 사례(인그레스, 이그레스/이스트-웨스트)를 처리하기 위해 3개의 서비스 VPC를 생성합니다. 각 VPC는 다음과 같이 생성되고 연계됩니다.

- 각 가용성 영역에 4개의 서브넷.
- 각 서브넷에 경로 테이블 1개.
- 보안 그룹 2개: 관리 및 데이터 경로.
- Transit 게이트웨이 1개.

참고 이 Transit 게이트웨이는 서비스 VPC 생성 중에 생성되어 게이트웨이에 연결됩니다. 이 게이트웨이는 다른 서비스 VPC와 함께 재사용할 수 있습니다.

- Transit 게이트웨이 경로 테이블.

참고 경로 테이블은 생성 프로세스의 일부로 서비스 VPC에 연결됩니다.

참고 AWS 게이트웨이 로드 밸런서(GWLB)는 GWLB의 초기 구축 후 가용성 영역 추가/제거를 지원하지 않습니다. 가용성 영역을 변경해야 하는 경우 서비스 VPC를 다시 구축해야 합니다. 자세한 내용은 AWS 설명서를 참조하십시오.

Azure 리소스

멀티 클라우드 방어에서 다음 리소스로 하나의 서비스 VNet을 생성했습니다.

- VNet 1개.
- 네트워크 보안 그룹 2개.

서비스 VNet CIDR 값은 스포크 VNet과 겹치지 않아야 합니다.

서비스 **VPC** 또는 **VNet** 생성

다음 절차에 따라 생성하려는 게이트웨이에 따라 서비스 VPC 또는 서비스 VNet을 생성합니다. 클라우드 서비스 제공자에게 있는 옵션을 확인하십시오.

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

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

단계 **3** 입력 매개변수 값:

- **Name(**이름**)** -서비스 VPC/VNet에 이름을 할당합니다.
- **CSP Account(CSP** 계정**)** - 서비스 VPC/VNet을 생성할 CSP 계정을 선택합니다.
- **Region(**지역**)** - 이 서비스 VPC 를 구축할 지역을 선택합니다.
- (Azure 전용) **CIDR Block(CIDR** 블록**)** - 서비스 VNet의 CIDR 블록입니다. 스포크(애플리케이션) VNet과 겹치지 않아야 합니다.
- (AWS/GCP 전용) **Datapath CIDR Block(**데이터 경로 **CIDR** 블록**)** - 멀티 클라우드 방어 게이트웨이 데이터 경로 서비스 VPC에 대한 CIDR 블록입니다. 이 CIDR 블록은 스포크(애플리케이션) VPC의 주소 범위와 중복되지 않아야 합니다.
- (AWS/GCP 전용) **Management CIDR Block(**관리 **CIDR** 블록**)** - 멀티 클라우드 방어 게이트웨이 관리 서비스 VPC에 대한 CIDR 블록입니다. 이 CIDR 블록은 스포크(애플리케이션) VPC의 주소 범위와 중복되지 않아야 합니다.
- **Availability Zones(**가용성 영역**)** - VPC를 생성하는 경우에는 하나 의 가용성 영역만 구성해야 합니다. VNet의 경우 멀티 클라우드 방어에서는 복원력을 위해 최소 두 개의 가용성 영역을 선택하는 것이 좋습니다.
- (Azure 전용) **Resource Group(**리소스 그룹**)** - 서비스 VNet을 구축할 리소스 그룹입니다.
- (AWS 전용)**Transit Gateway** - Transit Gateway는 중앙 허브를 통해 가상 프라이빗 클라우드와 온프레미스 네트워크를 연결합니다. 드롭다운 메뉴를 사용하여 이 VPC에 대한 기존 게이트웨이를 선택합니다. 선택할 기존 게

이트웨이가 없는 경우 **Create_new(**새로 생성**)**를 선택합니다. 이 옵션을 사용하면 멀티 클라우드 방어가 VPC 생성 프로세스의 일부로 하나를 생성할 수 있습니다.

- (AWS 전용) **Transit Gateway Name(Transit Gateway** 이름**)** - 새 트랜짓 게이트웨이를 생성하도록 선택한 경우 이 필드에 게이트웨이의 이름을 입력합니다.
- (AWS에만 해당) **Auto accept shared attachments(**공유 첨부 파일 자동 수락**)** - 새 트랜짓 게이트웨이를 생성하지 않고 다중 어카운트 허브 게이트웨이 구축에 이 VPC를 사용하려는 경우, 이 옵션을 선택합니다.
- **Use NAT Gateway(NAT** 게이트웨이 사용**)** - 모든 이그레스 트래픽이 NAT 게이트웨이를 통과하도록 하려면 이 옵션을 활성화합니다.

  주의 이 서비스 VPC를 구축하여 AWS에서 멀티 클라우드 방어 VPN 게이트웨이를 구축하려는 경우 이 NAT 게이트웨이 옵션을 활성화하지 마십시오.

다음에 수행할 작업

멀티 클라우드 방어 게이트웨이 추가.

멀티 클라우드 방어 게이트웨이 추가

다음 절차에 따라 클라우드 서비스 제공자용 멀티 클라우드 방어 게이트웨이을 추가합니다.

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

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

단계 **3** 게이트웨이를 추가할 클라우드 서비스 제공자를 선택합니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** 다음 정보를 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 유형**)** - Ingress(인그레스) 또는 Egress(이그레스)를 선택합니다.

  참고 이스트-웨스트 네트워크 플로우가 있는 경우 **Egress(**이그레스**)**를 선택합니다.

- **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) **NTP Profile(NTP** 프로파일**)** - 시간 동기화를 위한 NTP(Network Time Protocol).
- (선택 사항) **BGP profile(BGP** 프로파일**)** - VPN 연결을 지원하는 데 사용되는 BGP(Border Gateway Protocol). 멀티 클라우드 방어 게이트웨이를 사용하여 사이트 간 VPN 터널을 생성하려면 이 프로파일을 포함해야 합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 다음 매개변수를 제공합니다.

- **Security** (보안) - Egress(이그레스) 또는 Ingress(인그레스)를 선택합니다.

  참고 이스트-웨스트 네트워크 플로우가 있는 경우 **Egress(**이그레스**)**를 선택합니다.

- **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.
- **Resource Groups(**리소스 그룹**)** - 게이트웨이를 연결할 리소스 그룹을 선택합니다.
- **SSHPublic Key(SSH** 공용 키**)** - SSH 공개 키를 붙여넣습니다. 이 공개 키는 컨트롤러에서 디버그 및 모니터링을 위해 구축된 게이트웨이 인스턴스의 CLI에 액세스하는 데 사용됩니다.
- **VNet ID** - 게이트웨이와 연결할 VNet을 선택합니다.
- **User Assigned Identity ID(**사용자 할당 **ID)** - 이 게이트웨이와 연결할 클라우드 서비스 제공자 ID를 입력합니다.
- **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.
- **Disk Encryption(**디스크 암호화**)** - 드롭다운 메뉴에서 적절한 옵션을 선택합니다. 고객 관리 암호화 키의 경우, 사용자는 암호화 키의 리소스 ID를 입력해야 합니다.

단계 **8** **Availability Zone(**가용성 영역**)**, **Mgmt Subnet(**관리 서브넷**)** 및 **Datapath Subnet(**데이터 경로 서브넷**)**을 선택합니다. 사용 가능한 서브넷은 위에서 선택한 VPC 또는 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.

참고 일부 클라우드 서비스 제공자 지역은 다중 가용성 영역을 지원하지 않습니다. 이러한 지역에서는 게이트웨이 인스턴스가 단일 영역에만 구축됩니다.

단계 **9** (Azure 전용, 선택 사항) 애플리케이션과 동일한 VNet에서 멀티 클라우드 방어 게이트웨이을(를) 사용하여 분산형 모델을 구축하는 경우 다음을 완료해야 합니다.

- Azure 포털에서 경로 테이블을 추가하고 모든 서브넷에 경로 테이블을 연결합니다.
- **next-hop**을 게이트웨이 네트워크 로드 밸런서의 IP 주소로 사용하는 0.0.0.0/0에 대한 기본 경로를 추가합니다.

단계 **10** 고급 설정을 보려면 **Next(**다음**)**를 클릭합니다.

단계 **11** 기본적으로 멀티 클라우드 방어 게이트웨이는 사용 가능한 라우터의 공용 IP 사용을 활성화합니다. 이 기능을 활성화하지 않으려면 **Disable Public IP(**공용 **IP** 비활성화**)** 확인란을 선택합니다.

단계 **12** **Save(**저장**)**를 클릭합니다. 멀티 클라우드 방어는 게이트웨이를 구축합니다.

다음에 수행할 작업

스포크 VPC/VNet을 보호하기 전에 게이트웨이에 하나 이상의 규칙 집합을 연결해야 합니다. 자세한 내용은 규칙 집합 및 규칙 집합 그룹를 참조하십시오.

서비스 메뉴의 보안 스포크 **VPC/VNet**

다음 절차를 사용하여 서비스 메뉴에서 스포크 VPC 또는 스포크 VNet을 게이트웨이에 추가합니다.

시작하기 전에

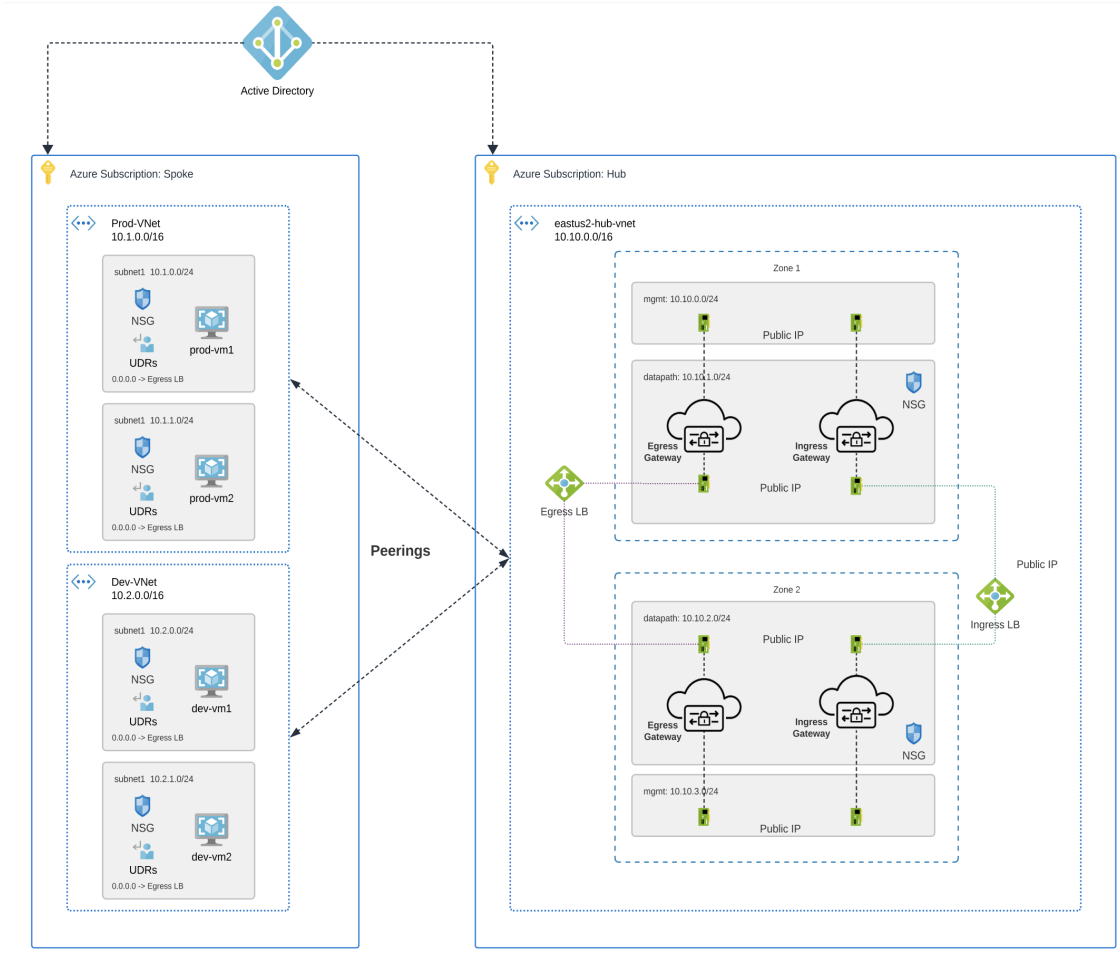
스포크 VPC 또는 VNet을 생성하고 할당하기 전에 다음 작업을 수행해야 합니다.

- AWS 및 GCP 계정에서는 게이트웨이를 추가하기 전에 원격 계정을 보호해야 합니다.
- Azure 환경에서는 스포크 VPC/VNet을 보호하기 전에 경로 테이블을 연결해야 합니다. 자세한 내용은 Azure 사용자 가이드의 "경로 테이블을 서브넷에 연결" 장을 참조하십시오.

중앙 집중식 모델에서 VPC로 AWS 스포크를 보호하는 경우, 멀티 클라우드 방어은(는) 서비스 VPC에 연결된 Transit 게이트웨이에 VPC를 연결합니다. VPC를 Transit 게이트웨이에 연결할 때 사용자는 ENI를 배치할 각 가용성 영역의 서브넷을 선택할 수 있습니다. 기본적으로 멀티 클라우드 방어은(는) Transit Gateway 연결에 대해 각 가용성 영역에서 서브넷을 무작위로 선택합니다.

VNet 페어링은 동일한 CSP 유형 내의 계정 간에 지원됩니다. 계정 내에서 그리고 계정 간에 스포크 VPC/VNet을 추가할 수 있습니다. Azure의 구독 간 스포크 VPC 피어링의 경우 동일한 앱 등록을 사용하여 CSP 계정을 온보딩해야 하며 구독은 동일한 Active Directory 내에 있어야 합니다.

그림 ***4: Azure*** 결합 허브 **-** 다중 구독



단계 **1** 멀티 클라우드 방어 컨트롤러 대시보드에서 **Manage(**관리**)** > **Service VPCs/VNets(**서비스 **VPC/VNets)**로 이동합니다.

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

단계 **3** 모든 스포크 VPC 또는 VNet을 추가하여 스포크 테이블을 보호합니다.

Spoke VNets for Current Account(현재 계정에 대한 스포크 **VNets)**에서 스포크 VPC 또는 VNets을 선택할 수 있습니다. 다른 계정의 스포크 VPC 또는 VNets를 추가하려면 **Spoke VNet for Other Accounts(**다른 계정에 대한 스포크 **VNet)**를 선택합니다.

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 **Gateway(**멀티 클라우드 게이트웨이를 통해 트래픽 전송**)** 확인란을 선택합니다.

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

단계 **7** **Save(**저장**)**를 클릭합니다.

게이트웨이 관리

관리자 > 게이트웨이에서 멀티 클라우드 방어 게이트웨이 및 통계를 봅니다. 이 페이지에서 게이트웨이를 검색 및 필터링하고, 각 게이트웨이와 관련된 클라우드 서비스 제공자, 현재 인스턴스 수 및 유형 등을 볼 수 있습니다.

특정 게이트웨이 환경에서 지원되는 활용 사례에 대한 자세한 내용은 지원되는 게이트웨이 활용 사례, 2 페이지를 참조하십시오.

멀티 클라우드 방어 게이트웨이 편집

활성화 또는 비활성화 여부에 상관없이 모든 상태의 게이트웨이를 편집할 수 있습니다. 다음 절차에 따라 기존 멀티 클라우드 방어 게이트웨이을 편집합니다.

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

단계 **2** 테이블에서 편집할 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Edit(**편집**)**를 선택합니다.

단계 **4** 필요에 따라 게이트웨이 구성을 수정합니다.

단계 **5** **Save(**저장**)**를 클릭하여 변경 사항을 확인합니다. 또는 변경을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

멀티 클라우드 방어 게이트웨이 업그레이드

멀티 클라우드 방어 게이트웨이는 자동 확장 자동 복구 PaaS(Platform-as-a-Service)로 작동하고 인라인 네트워크 기반 보안 시행 노드로 작동합니다. 기존 방화벽과 달리 멀티 클라우드 방어에서는 고객이 가상 방화벽을 구성하거나 고가용성 설정을 구성하거나 소프트웨어 설치를 관리할 필요가 없습니다.

멀티 클라우드 방어 게이트웨이 인스턴스는 효율적인 트래픽 처리 및 고급 보안 시행을 위해 단일 패스 데이터 경로 파이프라인을 통합하여 고도로 최적화된 소프트웨어에서 작동합니다. 각 게이트웨이 인스턴스는 정책 시행을 담당하는 "worker" 프로세스, 트래픽 배포 및 세션 관리를 담당하는 "distributor" 프로세스, 컨트롤러와 통신하는 "agent" 프로세스의 3가지 핵심 프로세스로 구성됩니다. 게이트웨이 인스턴스를 "데이터 경로 재시작"을 위해 "서비스 중"으로 원활하게 전환할 수 있으므로 트래픽 흐름을 중단하지 않고 원활한 업그레이드를 수행할 수 있습니다.

새 인스턴스가 새 이미지와 함께 회전합니다. 인스턴스는 완전히 가동되면 로드 밸런서(게이트웨이 인스턴스로의 플로우의 레이어 4 스프레이어)의 대상 풀에 배치됩니다. 기존 인스턴스는 이를 통과하는 기존 플로우에 대해 플로우 배수 모드 또는 플로우 시간 초과 모드가 됩니다. 새 플로우는 새 인스턴스에 적용됩니다. 시간 초과(Azure) 또는 플로우가 드레인(AWS)되면 컨트롤러에서 기존 인스턴스를 가져옵니다.

다음 절차를 사용하여 수행할 수 있습니다.

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

단계 **2** 업그레이드할 게이트웨이의 확인란을 선택합니다. 현재 하나의 항목만 선택할 수 있습니다.

단계 **3** **Actions(**작업**)** > **Upgrade(**업그레이드**)**를 선택합니다.

단계 **4** **Gateway Image(**게이트웨이 이미지**)** 목록에서 원하는 이미지를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 업그레이드에 필요한 클라우드 서비스 제공자 리소스 할당을 확인합니다.

단계 **7** 리소스 할당이 충분하면 **Yes(**예**)**를 클릭합니다. 리소스 할당이 충분하지 않은 경우 **No(**아니요**)**를 클릭하고 클라우드 서비스 제공자의 리소스 할당을 늘린 다음 돌아가서 업그레이드를 계속합니다.

Note 게이트웨이의 인스턴스 정보에서 업그레이드 진행 상황 및 새 게이트웨이 인스턴스를 볼 수 있습니다. 게이트웨이를 선택하고 Details(세부 사항) 창에서 **Instances(**인스턴스**)**를 확인합니다.

멀티 클라우드 방어 게이트웨이 중단

현재 게이트웨이 업데이트가 진행 중인 멀티 클라우드 방어 게이트웨이만 중단할 수 있습니다.

기존 멀티 클라우드 방어 게이트웨이를 중단하려면 다음 절차를 사용합니다.

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

단계 **2** 테이블에서 중단하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Abort(**중단**)**를 선택합니다.

단계 **4** 게이트웨이 중단을 확인하고 **Yes**(예)를 클릭합니다. 작업을 취소하려면 **No(**아니요**)**를 클릭합니다.

멀티 클라우드 방어 게이트웨이을 활성화

비활성화된 게이트웨이만 활성화할 수 있습니다. 다음 절차에 따라 활성화합니다.

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

단계 **2** 표에서 활성화하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Enable(**활성화**)**을 선택합니다.

단계 **4** 멀티 클라우드 방어은 게이트웨이 구성을 검증합니다. 검증에 성공하면 검토를 위해 업그레이드에 대한 현재 및 필수 리소스의 표가 생성됩니다. 게이트웨이 리소스 할당을 승인하는 경우 **Yes(**예**)**를 클릭하여 작업을 확인합니다.

다음에 수행할 작업

멀티 클라우드 방어 게이트웨이이 성공적으로 활성화될 때까지 몇 분 정도 기다립니다.

멀티 클라우드 방어 게이트웨이를 비활성화하고 연결된 사이트 간 VPN 터널을 삭제한 경우, 새 사이트 간 VPN 터널 연결을 생성해야 하거나 이전 VPN 터널 연결을 다시 생성한 다음 게이트웨이에 추가해야 합니다. 게이트웨이가 비활성화되면 멀티 클라우드 방어은 VPN 터널과 연결된 공용 IP 주소를 무시합니다. 게이트웨이 인스턴스에 대해 새 IP를 설정하려면 새 터널 연결을 생성해야 합니다.

멀티 클라우드 방어 게이트웨이 비활성화

멀티 클라우드 방어 게이트웨이가 현재 활성화되어 있는 경우에만 비활성화할 수 있습니다. 이미 비활성화된 게이트웨이는 비활성화할 수 없습니다.

다음 절차에 따라 멀티 클라우드 방어 게이트웨이를 비활성화합니다.

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

단계 **2** 표에서 중단하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Disable(**비활성화**)**를 선택합니다.

단계 **4** 게이트웨이를 비활성화할 것인지 확인하고 **Yes**(예)를 클릭합니다. 이 작업을 취소하려면 **No(**아니요**)**를 클릭합니다.

다음에 수행할 작업

게이트웨이가 성공적으로 비활성화될 때까지 몇 분 정도 기다립니다.

게이트웨이를 완전히 비활성화하려면 게이트웨이와 연계된 모든 사이트 간 VPN 터널을 삭제해야 합니다.

멀티 클라우드 방어 게이트웨이 내보내기

다음 절차에 따라 멀티 클라우드 방어 게이트웨이의 구성을 내보냅니다.

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

단계 **2** 표에서 내보내려는 멀티 클라우드 방어 게이트웨이을 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Export(**내보내기**)**를 선택합니다.

단계 **4** 멀티 클라우드 방어이 내보내기 마법사를 생성합니다.

단계 **5** **Download(**다운로드**)**를 클릭하여 terraform을 로컬로 다운로드하거나 아래로 스크롤하여 **Copy Code(**코드 복사**)**를 클릭하여 JSON 리소스를 복사합니다.

단계 **6** Terraform 스크립트에 수동으로 붙여넣습니다.

단계 **7** terraform 프롬프트에서 창 하단에 있는 명령을 실행합니다. `terraform import "ciscomcd_gateway"."object-name" <object name>`.

단계 **8** Terraform 프롬프트의 프롬프트에 따라 작업을 완료합니다. 멀티 클라우드 방어에서 내보내기 창을닫습니다**.** 대시보드에 더 이상 단계가 없습니다.

멀티 클라우드 방어 게이트웨이 삭제

다음 절차에 따라 멀티 클라우드 방어 게이트웨이을 삭제합니다. 이 작업은 게이트웨이 비활성화와 다릅니다.

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

단계 **2** 표에서 중단하려는 멀티 클라우드 방어 게이트웨이를 선택하여 강조 표시합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 확장하고 **Delete(**삭제**)**를 선택합니다.

단계 **4** 작업을 확인하고 **Yes(**예**)**를 클릭합니다. 삭제 작업을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

다음에 수행할 작업

이 게이트웨이와 연결된 사이트 간 VPN 터널 연결은 게이트웨이 표에서 성공적으로 삭제된 후에 삭제하는 것이 좋습니다.