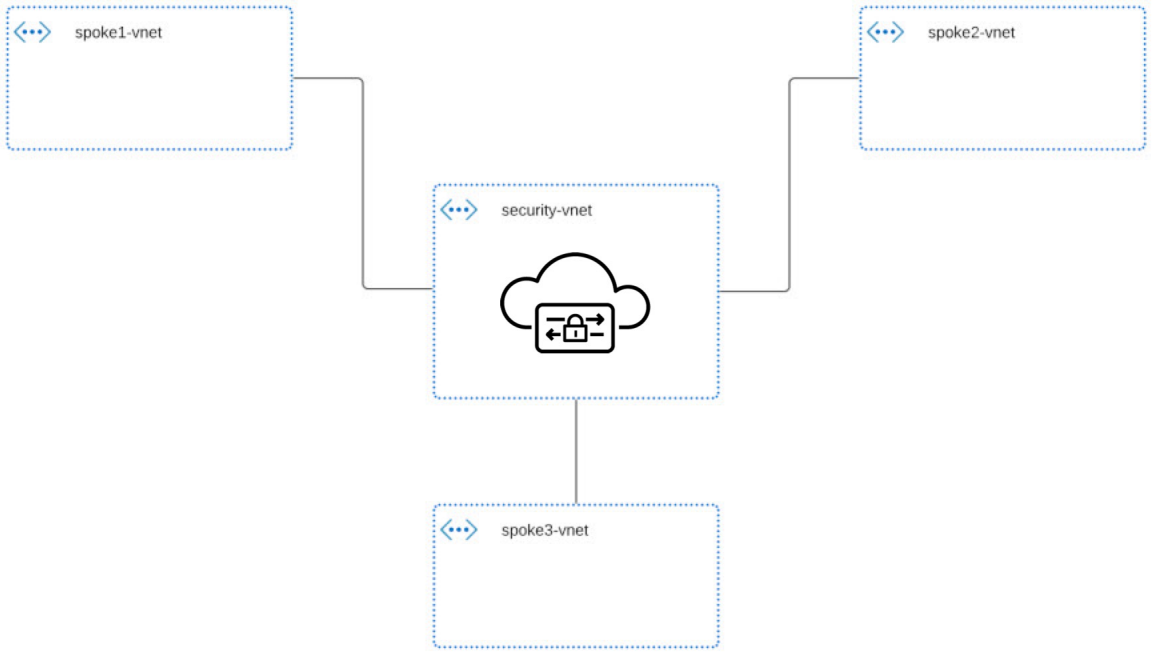
Azure

서비스 VNet

Azure 서비스 VNet

중앙 집중식 구축의 경우 멀티 클라우드 방어 게이트웨이이(가) 새 서비스 VNet에 구축됩니다. 이 VNet을 서비스 VNet이라고 하며 다른 스포크(애플리케이션) VNet과 피어링되어 아래와 같이 허브 앤 스포크 모델을 생성합니다.



멀티 클라우드 방어은(는) 서비스 VNet 생성을 오케스트레이션하고 스포크 VNet을 사용하여 VNet 피어링을 수행합니다. 또한 멀티 클라우드 방어에서는 검사를 위해 트래픽을 서비스 VNet으로 라우팅하도록 스포크 VNet에서 라우팅을 업데이트하는 기능을 제공합니다. 스포크 VNet에서 멀티 클라우드 방어을(를) 사용하여 라우팅을 변경하는 방법에 대한 지침은 허브 모드에서 스포크 VPC 관리(보호), on page 2의 내용을 참조하십시오.

서비스 VNet 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 VNet의 이름입니다.
CSP 계정	서비스 VNet을 생성하는 AzureSubscription입니다. 이 구독은 멀티 클라우드 방어 컨트롤러에 온보딩해야 합니다.
지역	서비스 VNet을 구축할 Azure 지역입니다.
CIDR 블록	서비스 VNet에 대한 CIDR 차단입니다. 스포크(애플리케이션) VNet과 겹치지 않아야 합니다.
가용성 영역	탄력성을 위해 2개 이상을 선택하는 것이 좋습니다. 모든 Azure 지역에 다중 AZ가 있는 것은 아닙니다.
리소스 그룹	서비스 VNet을 구축할 리소스 그룹입니다.

Note

- 서비스 VNet은 다음으로 구성됩니다.
  - Vnet
  - 2개의 NSG
- 서비스 VNet CIDR은 스포크 VNet과 겹치지 않아야 합니다.

허브 모드에서 스포크 VPC 관리(보호)

멀티 클라우드 방어에서는 서비스 VNet의 모든 오케스트레이션을 처리하고 모든 스포크 VNet에 대한 VNet 피어링을 수행할 수 있습니다. 멀티 클라우드 방어은(는) 경로를 변경할 수 있어 검사를 위해 스포크 VNet 트래픽이 멀티 클라우드 방어 게이트웨이(으)로 라우팅됩니다. 이는 워크로드를 매우 쉽게 구축하고 보호할 수 있는 완전 관리형 솔루션입니다.

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 VNet을 보호하려면 스포크 VNet과 서비스 VNet 간에 VNet 피어링을 수행해야 합니다. 이를 통해 멀티 클라우드 방어은(는) 멀티 클라우드 방어에서 검사할 스포크 VNet 트래픽에 대한 라우팅 및 VNet 피어링을 오케스트레이션할 수 있습니다.

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

- 멀티 클라우드 방어 서비스 VNet과 스포크 VNet 간에 VNet 피어링 생성
- 멀티 클라우드 방어 게이트웨이을(를) 가리키는 스포크 경로 테이블의 기본 경로 추가/업데이트

VNet을 서비스 VNet에 연결하는 방법에는 두 가지가 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 **Manage Spoke VPC/VNet(**스포크 **VPC/VNet** 관리**)**을 클릭합니다.
단계 **3** 스포크 테이블에 모든 스포크 VNet을 추가합니다.
단계 **4** Route Tables(경로 테이블) 열에서 View/Edit(보기/편집) 링크를 클릭합니다.
단계 **5** 검사를 위해 기본 경로를 멀티 클라우드 방어 게이트웨이(으)로 업데이트할 경로 테이블을 선택합니다.
단계 **6** **Save Locally(**로컬로 저장**)**를 클릭합니다.
단계 **7** **Save(**저장**)**를 클릭합니다.

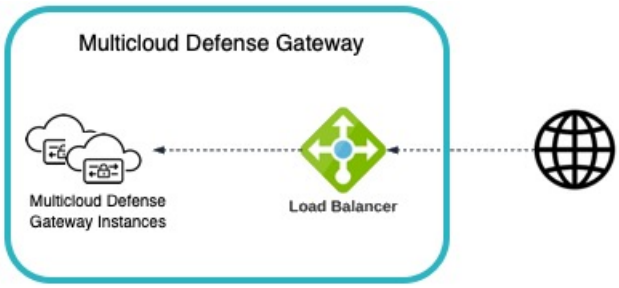
재고 목록 메뉴에서 스포크 VPC 추가

단계 **1** **Manage(**관리**)** > **Cloud Accounts(**클라우드 계정**)** > **Inventory(**재고 목록**)**로 이동합니다.
단계 **2** VPC/VNets를 클릭합니다. 그러면 클라우드 계정의 모든 VNet이 나열됩니다.
단계 **3** VNet을 보호하려면 **Secure(**보안**)** 버튼을 클릭합니다.
단계 **4** Service VNet(서비스 VNet)을 선택합니다.
단계 **5** 검사를 위해 기본 경로를 멀티 클라우드 방어 게이트웨이(으)로 업데이트할 경로 테이블을 선택합니다.
단계 **6** **Save(**저장**)**를 클릭합니다.

Azure 중앙 집중식 인그레스 보호

멀티 클라우드 방어 게이트웨이은(는) 인터넷 연결 애플리케이션을 보호하기 위해 VNet에 구축됩니다. 중앙 집중식 모델의 경우 서비스 VNet에 게이트웨이를 구축합니다. 게이트웨이는 역방향 프록시 역할을 합니다. 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.

멀티 클라우드 방어 게이트웨이은(는) 멀티 클라우드 방어 게이트웨이 인스턴스를 전면에 배치하는 데 사용되는 로드 밸런서로 구성됩니다. 따라서 보다 확장 가능한 설계가 가능하며 모든 게이트웨이 인스턴스 간에 트래픽의 로드 밸런싱이 가능합니다.



게이트웨이 추가

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.
- **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.
- **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 **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.

Note Azure 포털을 사용하여 VM 인스턴스 페이지를 보고 생성된 게이트웨이 인스턴스를 확인합니다. VM에는 멀티 클라우드 방어(으)로 시작하는 이름 태그가 있습니다.

Check Load Balancers(로드 밸런서 확인**)** 섹션에서 내부 네트워크 로드 밸런서가 생성되었는지 확인합니다.

관련 주제: 고급 설정.

고급 설정

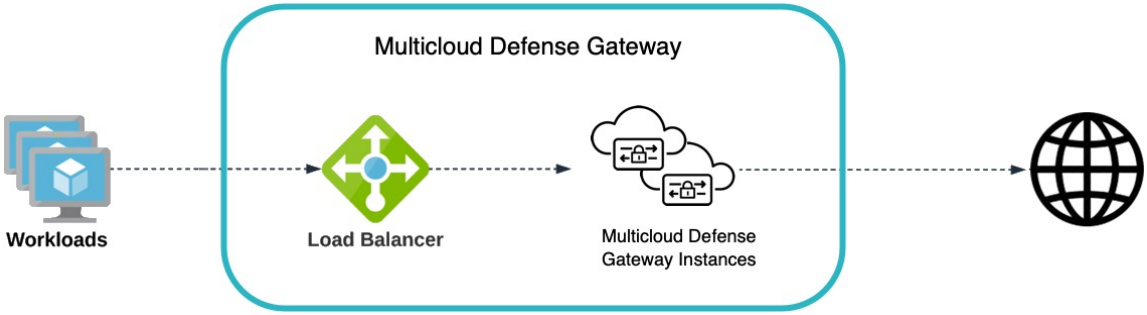
Advanced Settings(고급 설정)를 사용하면 멀티 클라우드 방어 게이트웨이에서 사용자 지정 기본 설정을 사용할 수 있습니다. 이러한 설정 중 일부는 게이트웨이 구축 후 편집하지 못할 수 있습니다.

매개변수	설명
UseInternal LoadBalancer	이 옵션은 멀티 클라우드 방어 게이트웨이 구축 시 내부 로드 밸런서를 사용합니다. 이는 일반적으로 애플리케이션이 공개 액세스용이 아닌 비공개용으로 사용되는 경우에 사용됩니다.
ManagementDNS Server	사용자는 기본 클라우드 DNS 대신 지정된 DNS 서버를 가리키도록 멀티 클라우드 방어 게이트웨이을(를) 구성할 수 있습니다. DNS가 변경된 경우 DNS가 다음 URL을 확인할 수 있는지 확인하십시오. • prod1-dashboard.vtxsecurityservices.com • prod1-apiserver.vtxsecurityservices.com • prod1-watchserver.vtxsecurityservices.com 이러한 URL은 멀티 클라우드 방어 게이트웨이이(가) 작동하는지 확인하는 데 필요합니다. * Azure DNS 설정은 새 게이트웨이 인스턴스를 구축할 때만 설정할 수 있습니다. 편집해야 하는 경우 게이트웨이를 비활성화하여 DNS를 편집하십시오.

Azure 중앙 집중식 이그레스/이스트-웨스트 보호

멀티 클라우드 방어 게이트웨이은(는) 발신 트래픽을 보호하기 위해 VNet에 구축됩니다. 중앙 집중식 모델의 경우 게이트웨이는 서비스 VNet에 구축됩니다. 게이트웨이는 정방향 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.

멀티 클라우드 방어 게이트웨이은(는) 멀티 클라우드 방어 게이트웨이 인스턴스를 전면에 배치하는 데 사용되는 로드 밸런서로 구성됩니다. 따라서 보다 확장 가능한 설계가 가능하며 모든 게이트웨이 인스턴스 간에 트래픽의 로드 밸런싱이 가능합니다.



게이트웨이 추가

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.

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 **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 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 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.
- **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 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.

Note Azure 포털을 사용하여 VM 인스턴스 페이지를 보고 생성된 게이트웨이 인스턴스를 확인합니다. VM에는 멀티 클라우드 방어(으)로 시작하는 이름 태그가 있습니다.

Check Load Balancers(로드 밸런서 확인**)** 섹션에서 내부 네트워크 로드 밸런서가 생성되었는지 확인합니다.

단계 **9** (선택 사항) 분산형 모델을 구축하는 경우(애플리케이션과 동일한 VNet의 멀티 클라우드 방어 게이트웨이) 스포크 **VNet** 관리에 따라 VNet을 보호하십시오. 분산형 모델의 경우 VNet의 앱/서브넷 트래픽을 멀티 클라우드 방어 게이트웨이(으)로 라우팅해야 합니다.

- Azure 포털에서 경로 테이블을 추가합니다.
- 경로 테이블을 모든 서브넷과 연결합니다.
- next-hop을 멀티 클라우드 방어 게이트웨이 네트워크 로드 밸런서의 IP 주소로 사용하는 0.0.0.0/0에 대한 기본 경로를 추가합니다.

고급 설정

Advanced Settings(고급 설정)를 사용하면 멀티 클라우드 방어 게이트웨이에서 사용자 지정 기본 설정을 사용할 수 있습니다. 이러한 설정 중 일부는 게이트웨이 구축 후 편집하지 못할 수 있습니다.

매개변수	설명
ManagementDNS Server	사용자는 기본 클라우드 DNS 대신 지정된 DNS 서버를 가리키도록 멀티 클라우드 방어 게이트웨이을(를) 구성할 수 있습니다. DNS가 변경된 경우 DNS가 다음 URL을 확인할 수 있는지 확인하십시오. • prod1-dashboard.vtxsecurityservices.com • prod1-apiserver.vtxsecurityservices.com • prod1-watchserver.vtxsecurityservices.com 이러한 URL은 멀티 클라우드 방어 게이트웨이이(가) 작동하는지 확인하는 데 필요합니다. Azure DNS 설정은 새 게이트웨이 인스턴스를 구축할 때만 설정할 수 있습니다. 이 설정을 편집하려면 게이트웨이를 비활성화하십시오.