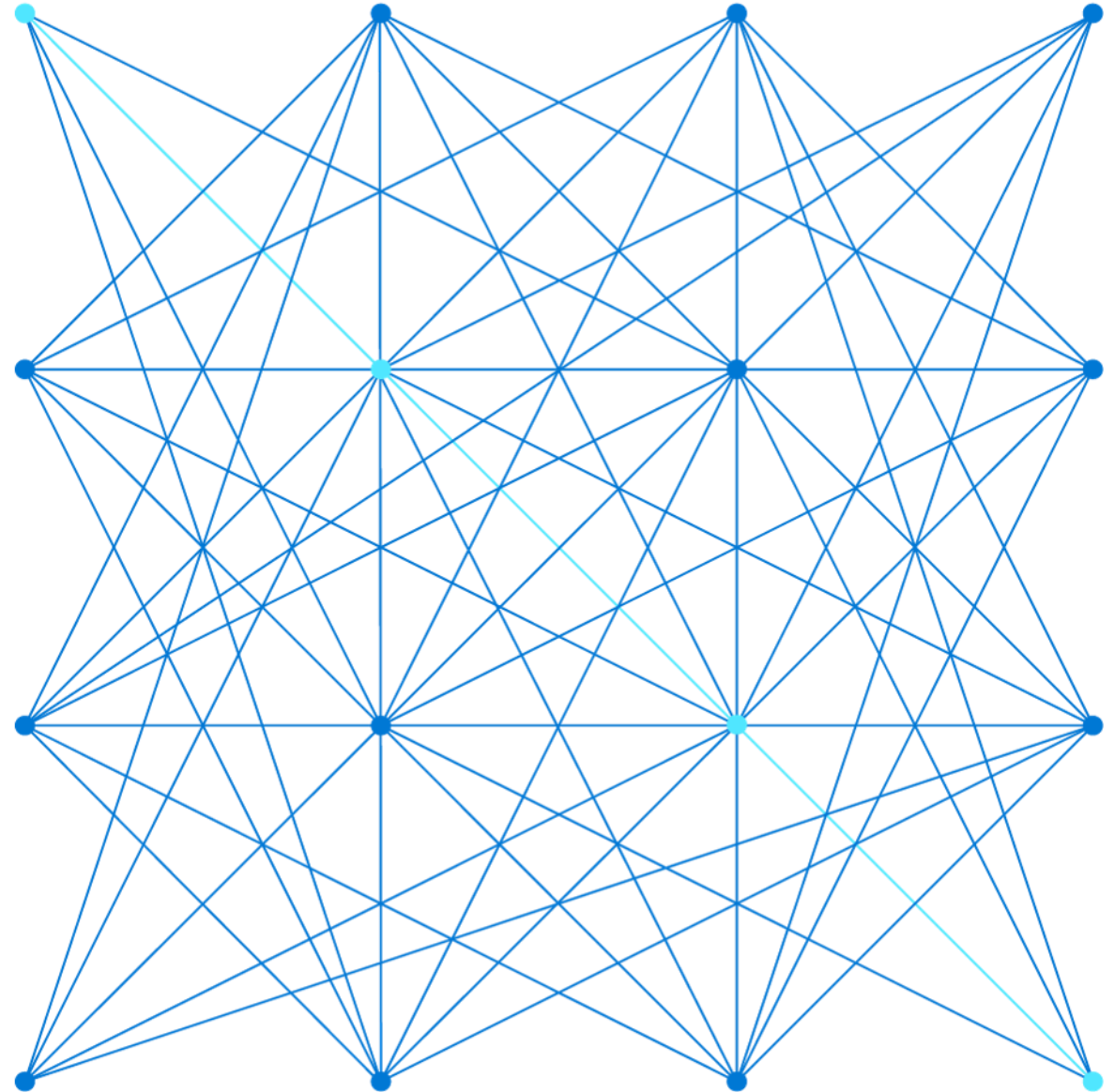
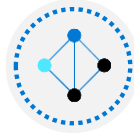


# AZ-104T00A

## 네트워크 트래픽 관리



# 네트워크 트래픽 관리 소개



네트워크 라우팅 및 엔드포인트 구성



Azure Load Balancer 구성



Application Gateway 구성

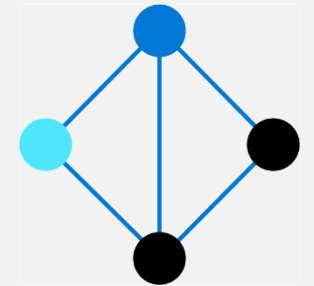


Network Watcher 구성



랩 06 – 트래픽 관리 구현

# 네트워크 라우팅 및 엔드포인트 구성



# 네트워크 라우팅 및 엔드포인트 구성 소개



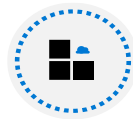
시스템 경로 검토



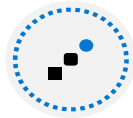
사용자 정의 경로 식별



데모 - 사용자 지정 라우팅 테이블  
• 라우팅 예 살펴보기



서비스 엔드포인트 사용 확인



Private Link 사용 식별

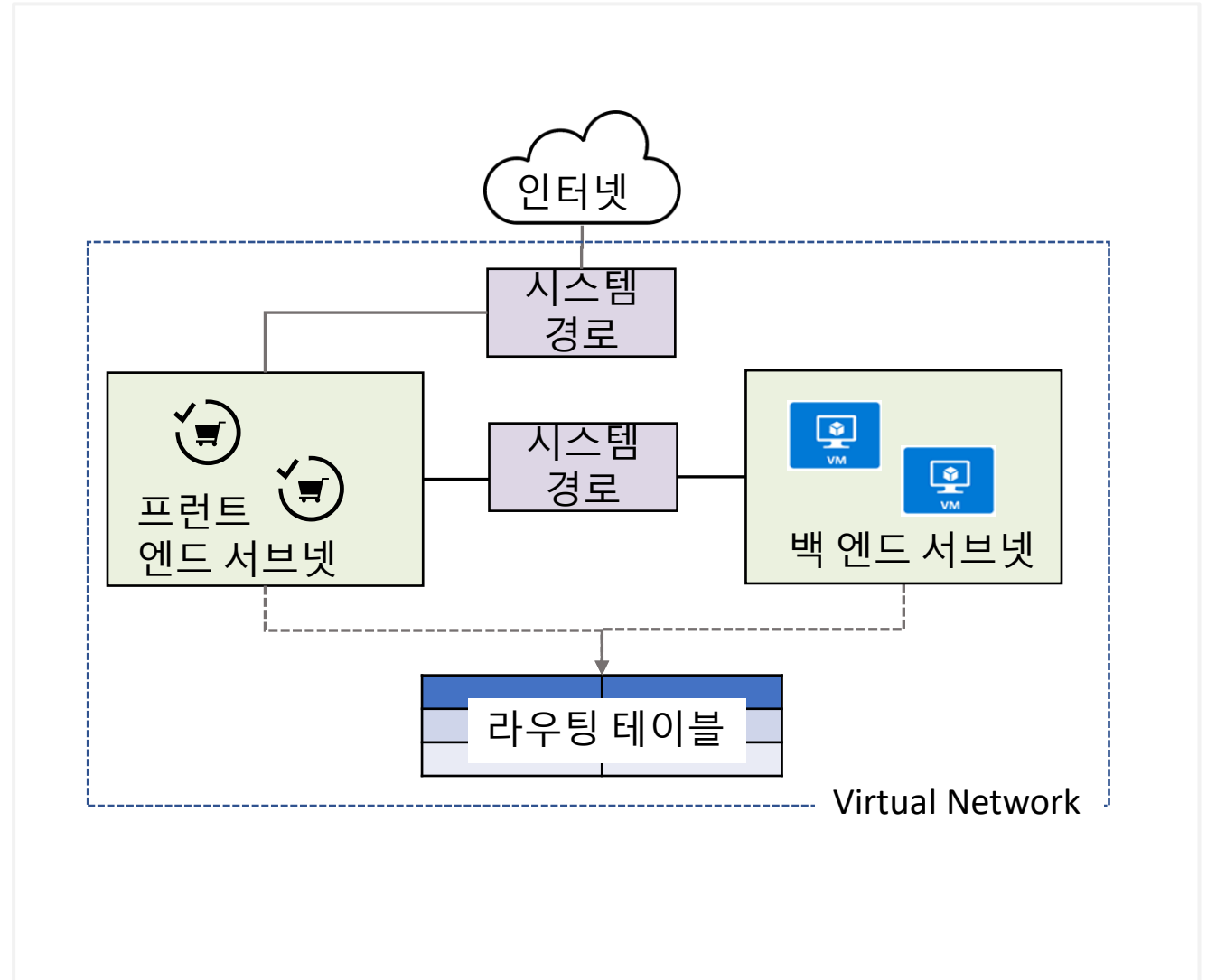


요약 및 리소스

# 시스템 경로 검토

시스템은 가상 머신, 온-프레미스 네트워크, 인터넷 간의 직접 네트워크 트래픽을 라우팅합니다.

- 동일한 서브넷에 있는 VM 간의 트래픽
- 동일한 가상 네트워크의 서로 다른 서브넷에 포함된 VM 간
- VM에서 인터넷으로 향하는 데이터 흐름
- VNet 간 VPN을 사용하는 VM 간 통신
- VPN Gateway를 통한 사이트 간 및 ExpressRoute 통신

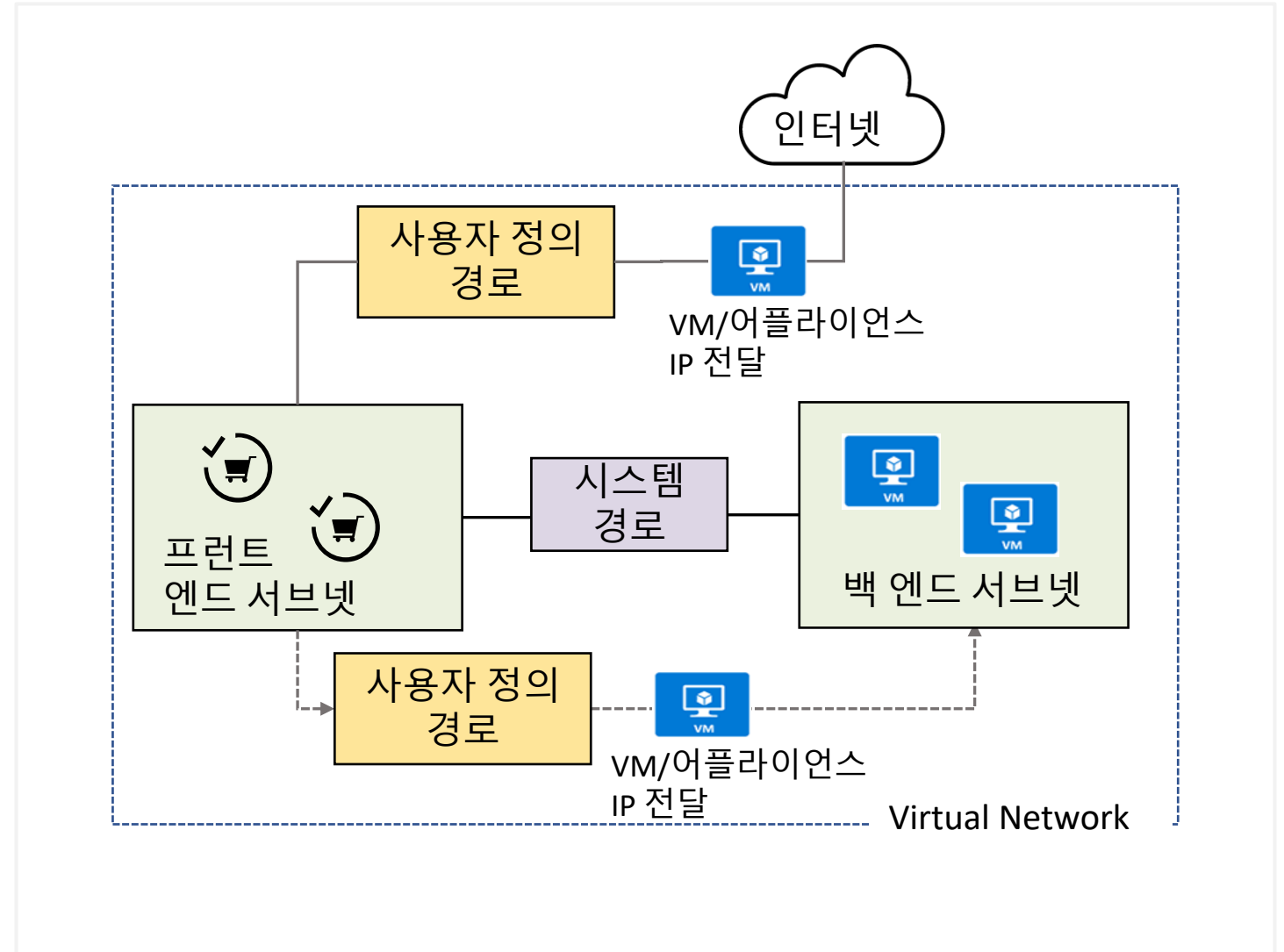


# 사용자 정의 경로 식별

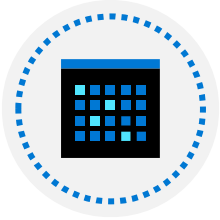
경로 테이블에는 가상 네트워크에서 패킷 라우팅 방법을 지정하는 규칙 집합(경로)이 포함되어 있습니다.

사용자 정의 경로는 트래픽 흐름의 다음 홉을 지정하는 경로를 정의하여 네트워크 트래픽을 제어하는 사용자 지정 경로입니다.

다음 홉은 가상 네트워크 게이트웨이, 가상 네트워크, 인터넷 또는 가상 어플라이언스일 수 있습니다.



# 데모 – 사용자 지정 라우팅 테이블



경로 테이블 만들기

---



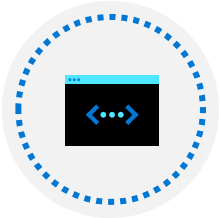
경로 추가

---



서브넷에 경로 테이블 연결

---



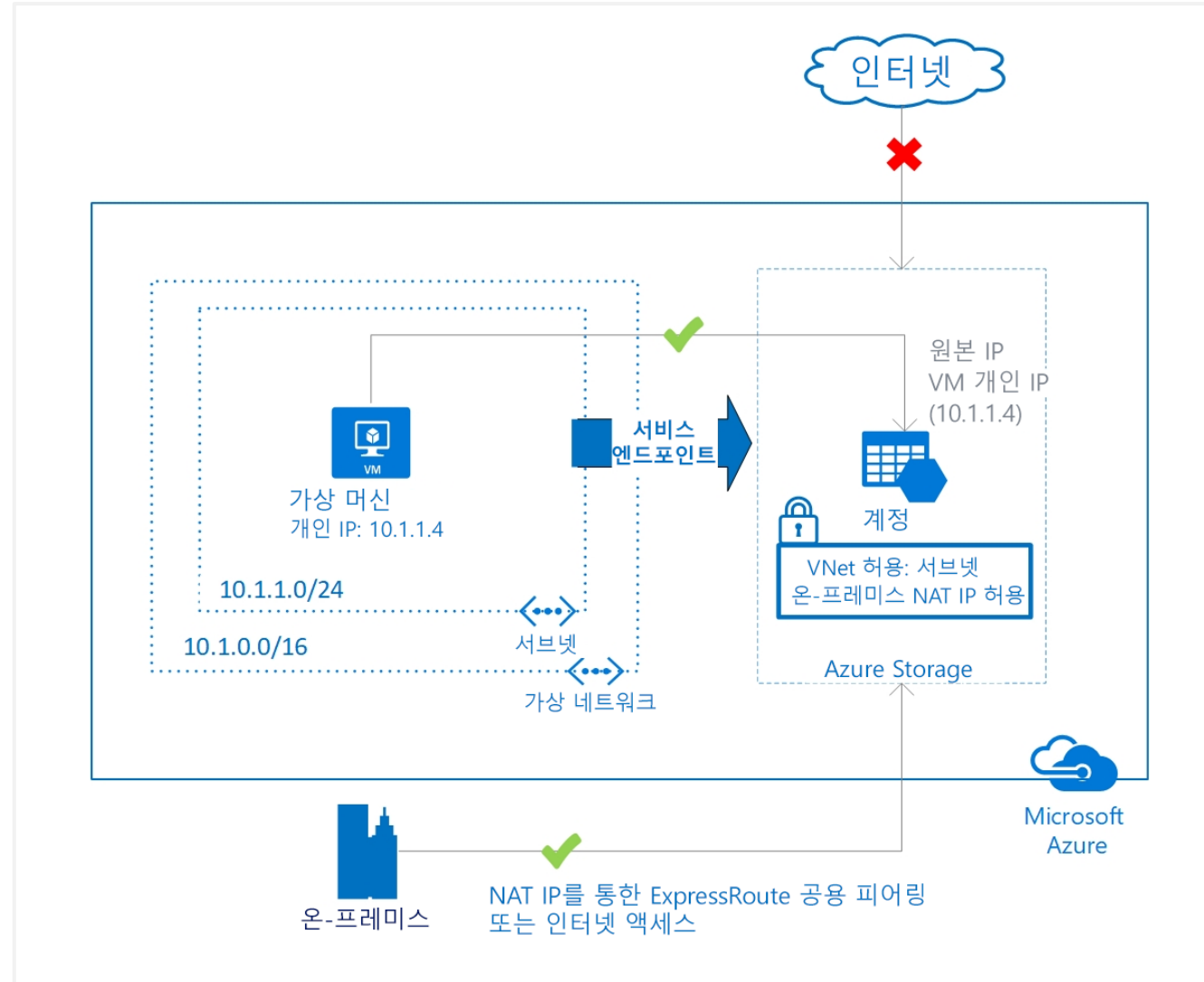
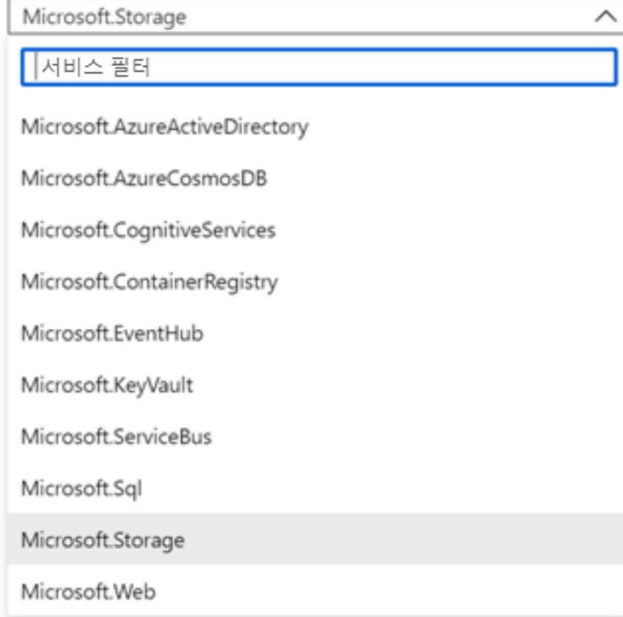
PowerShell을 사용하여 라우팅 정보 보기(선택 사항)

# 서비스 엔드포인트 사용 확인

엔드포인트는 특정 서비스에 대한 네트워크 액세스를 제한합니다. 서비스 엔드포인트를 추가하는 작업은 완료하는데 최대 15분이 걸릴 수 있습니다.

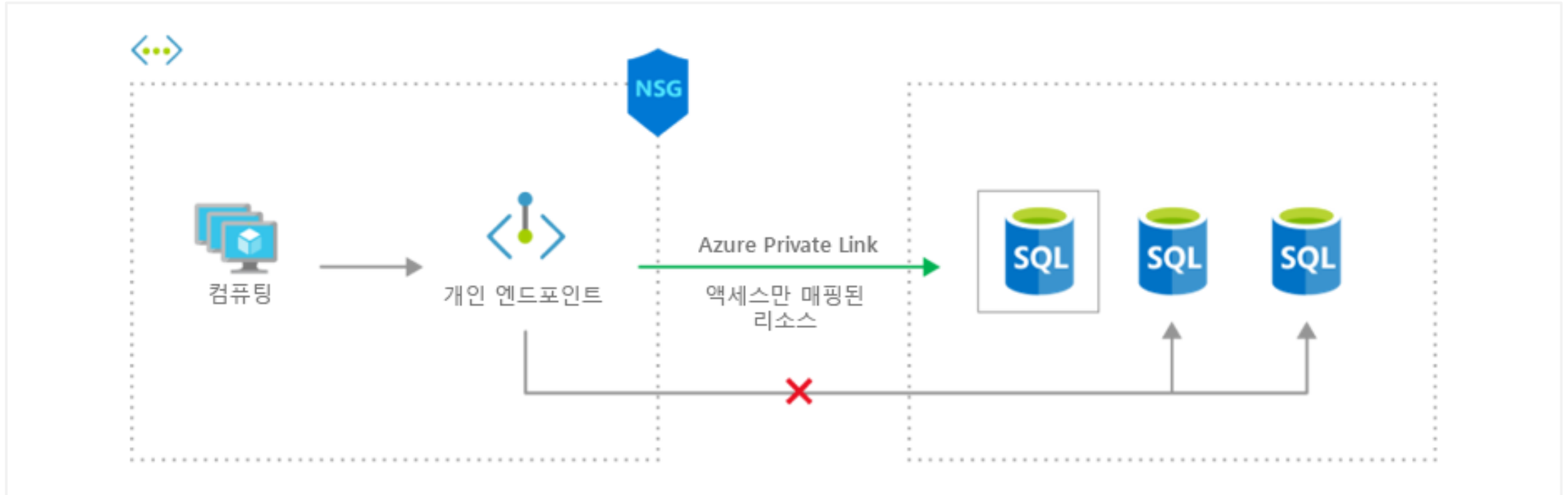
## 서비스 엔드포인트 추가

서비스 \*





# Private Link 사용 식별



Azure의 서비스에 대한 프라이빗 연결. 트래픽은 퍼블릭 인터넷 액세스 없이 Microsoft 네트워크에 남습니다.

온-프레미스 및 피어링된 네트워크와의 통합

네트워크 내에서 보안 인시던트가 발생하면 매핑된 리소스만 액세스할 수 있습니다.

# 요약 및 리소스 - 네트워크 라우팅 및 엔드포인트 구성

지식 점검 문제

Microsoft Learn 모듈([docs.microsoft.com/ko-kr/Learn](https://docs.microsoft.com/ko-kr/Learn))



[경로를 사용하여 Azure 배포에서 트래픽 흐름 관리 및 제어\(샌드박스\)](#)

---

[Azure Private Link 소개](#)

---

샌드박스는 실습 연습을 나타냅니다.

# Azure Load Balancer 구성



# Azure Load Balancer 구성 소개



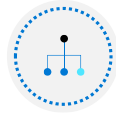
Load Balancer 솔루션 선택



공용 부하 분산 장치 구현



내부 부하 분산 장치 구현



Load Balancer SKU 결정



백 엔드 풀 만들기



부하 분산 장치 규칙 만들기



세션 지속성 구성(선택 사항)

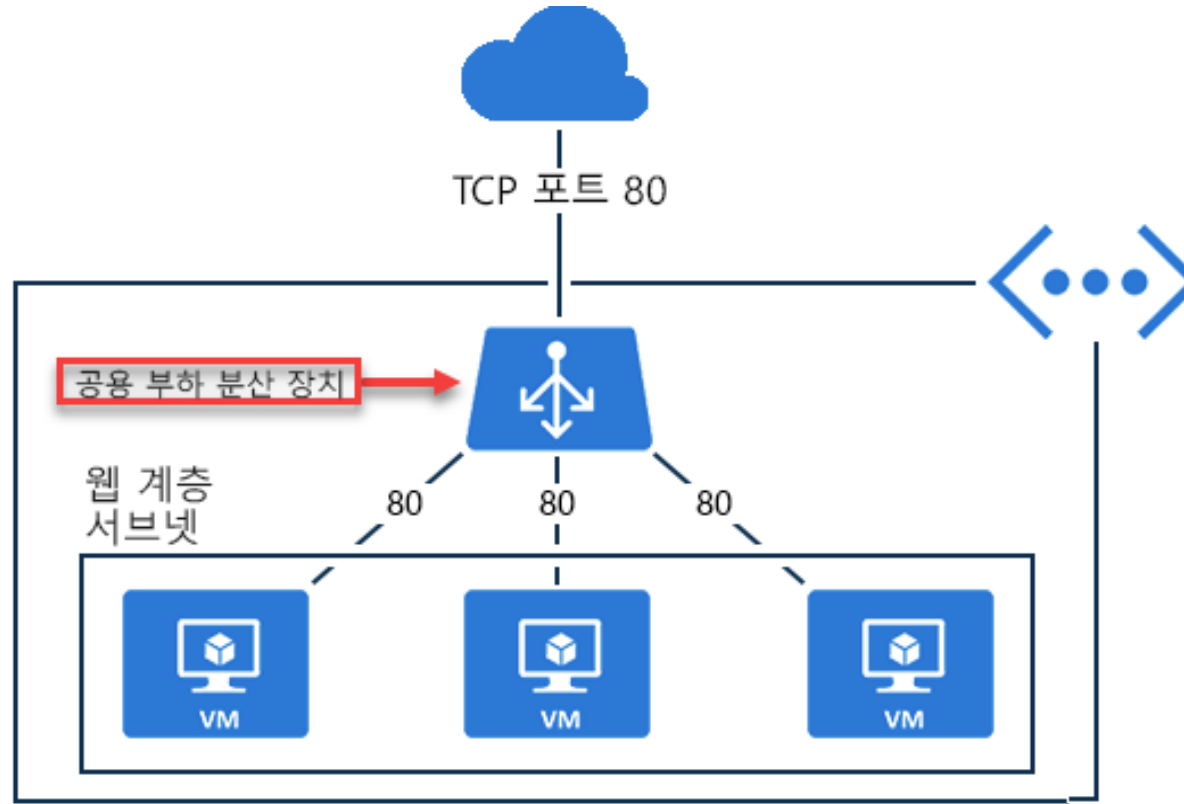


요약 및 리소스

# Load Balancer 솔루션 선택

기능	Application Gateway	Front Door	Load Balancer	Traffic Manager
사용량	웹 애플리케이션 방화벽을 사용하여 애플리케이션 보안을 강화하면서 애플리케이션 서버 팜의 배달을 최적화합니다.	글로벌 마이크로 서비스 기반 웹 애플리케이션을 위한 스케일링 가능하고 보안이 강화된 배달 지점입니다.	애플리케이션 또는 서버 엔드포인트에 대한 인바운드 및 아웃바운드 연결 및 요청의 균형을 조정합니다.	고가용성 및 응답성을 제공하면서 글로벌 Azure 지역 전반의 서비스에 트래픽을 최적으로 분산합니다.
프로토콜	HTTP, HTTPS, HTTP2	HTTP, HTTPS, HTTP2	TCP, UDP	모두
프라이빗	예		예	
전역		예		예
Env	Azure, 비 Azure 클라우드, 온-프레미스	Azure, 비 Azure 클라우드, 온-프레미스	Azure	Azure, 비 Azure 클라우드, 온-프레미스
보안	WAF	WAF, NSG	NSG	

# 공용 부하 분산 장치 구현



공용 IP 주소와 들어오는 트래픽의 포트 번호가 VM의 개인 IP 주소 및 포트 번호와 상호 매핑됩니다.

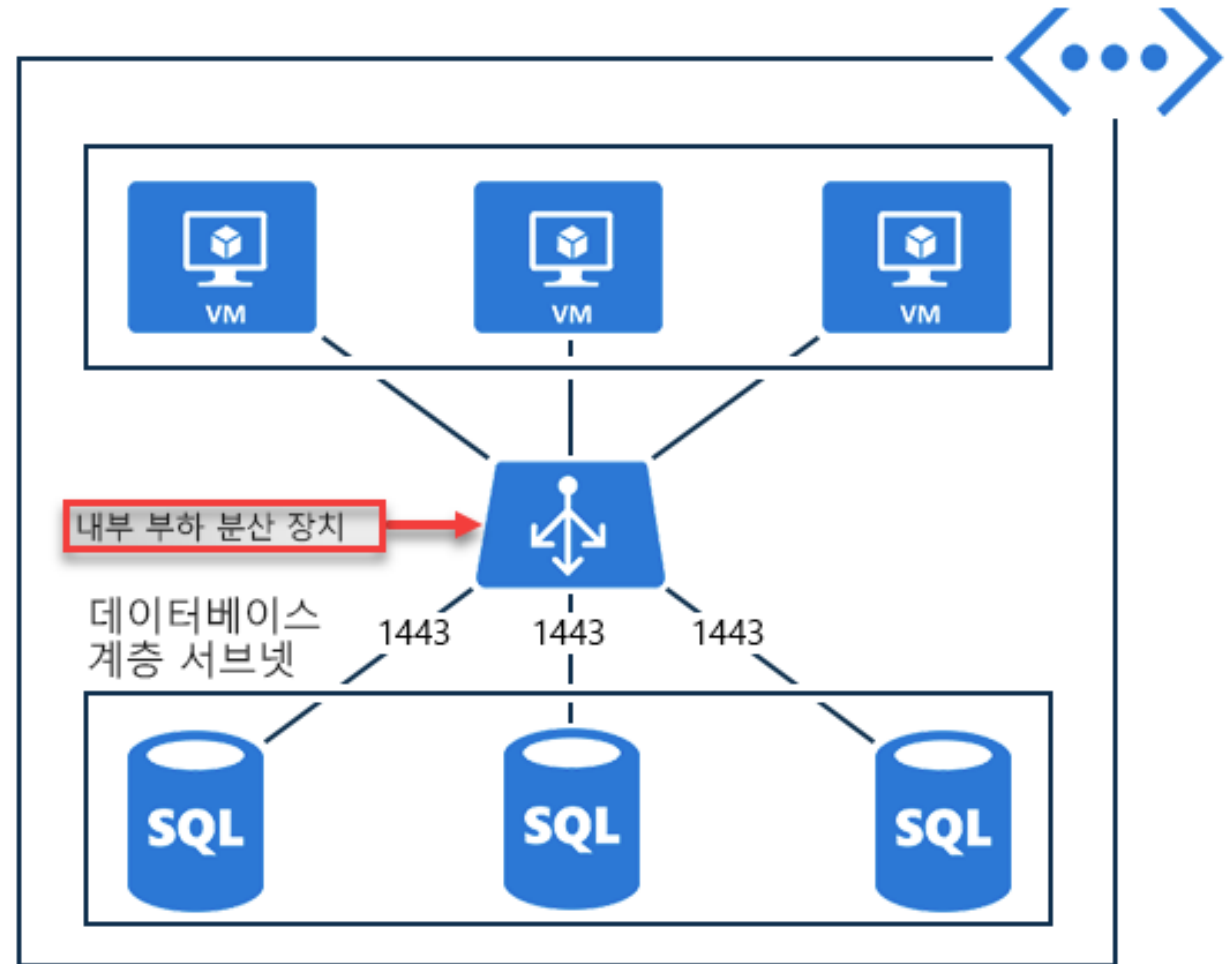
부하 분산 규칙을 적용하여 여러 VM 또는 서비스 간에 트래픽을 분산합니다.

# 내부 부하 분산 장치 구현

가상 네트워크 내에 있거나 VPN을 사용하여 Azure 인프라에 액세스하는 리소스로만 트래픽을 전송합니다.

프런트 엔드 IP 주소와 가상 네트워크는 인터넷 엔드포인트에 직접 노출되지 않습니다.

가상 네트워크 내에서 프리미엄 간 가상 네트워크, 다중 계층 애플리케이션, 사업 부문 애플리케이션에 부하 분산을 사용할 수 있습니다.



# Load Balancer SKU 결정

기능	기본 SKU	표준 SKU
백 엔드 풀	최대 300개 인스턴스	최대 1,000개 인스턴스
상태 프로브	TCP, HTTP	TCP, HTTP, HTTPS
가용성 영역	사용할 수 없음	인바운드 및 아웃바운드 트래픽에 대한 영역 중복 및 영역 프론트 엔드가 있습니다.
여러 프론트 엔드	인바운드 전용	인바운드 및 아웃바운드
기본적으로 보안 적용	기본적으로 업니다.NSG는 선택 사항입니다.	NSG에서 허용하지 않는 한 인바운드 흐름으로 종결됩니다. 가상 네트워크에서 내부 부하 분산 장치에 대한 내부 트래픽은 허용됩니다.
SLA	사용할 수 없음	99.99%

인스턴스 정보

이름 \* lb01 ✓

지역 \* (US) 미국 동부 2 ▼

형식 \* ① ☒ 내부 ☐ 공개

SKU \* ① ☒ 표준 ☐ 기본

가상 네트워크를 구성합니다.

가상 네트워크 \* ① vnet01 ▼

서브넷 \* subnet01 (10.1.0.0/24) ▼  
[서브넷 구성 관리](#)

IP 주소 할당 \* ☐ 정적 ☒ 동적



# 백 엔드 풀 만들기

설정

백엔드 풀

★ 이름

cesbackendpool

관련 ⓘ

연결되지 않음

연결되지 않음

가용성 세트

단일 가상 머신

가상 머신 확장 집합

SKU	백 엔드 풀 엔드포인트
기본 SKU	단일 가용성 집합 또는 VM 확장 집합의 VM
표준 SKU	VM, 가용성 집합, VM 확장 집합의 혼합을 포함한 단일 가상 네트워크의 모든 VM

트래픽을 분산하기 위해 부하 분산 장치에 연결된 가상 NIC의 IP 주소가 백 엔드 주소 풀에 포함됩니다.

# 부하 분산 장치 규칙 만들기

백 엔드 풀 및 포트 조합 집합에 프런트 엔드 IP 및 포트 조합을 매핑합니다.

규칙은 NAT 규칙과 결합할 수 있습니다.

NAT 규칙이 VM(또는 네트워크 인터페이스)에 명시적으로 연결되어 대상에 대한 경로를 완료합니다.

부하 분산 규칙 추가 ...

lb01

이름 \*

IP 버전 \* ☒ IPv4 ☐ IPv6

프런트 엔드 IP 주소 \* ①

☐ HA 포트 ①

프로토콜 ☒ TCP ☐ UDP

포트 \*

백 엔드 포트 \* ①

백 엔드 풀 \* ①

상태 프로브 \* ①   
[새로 만들기](#)

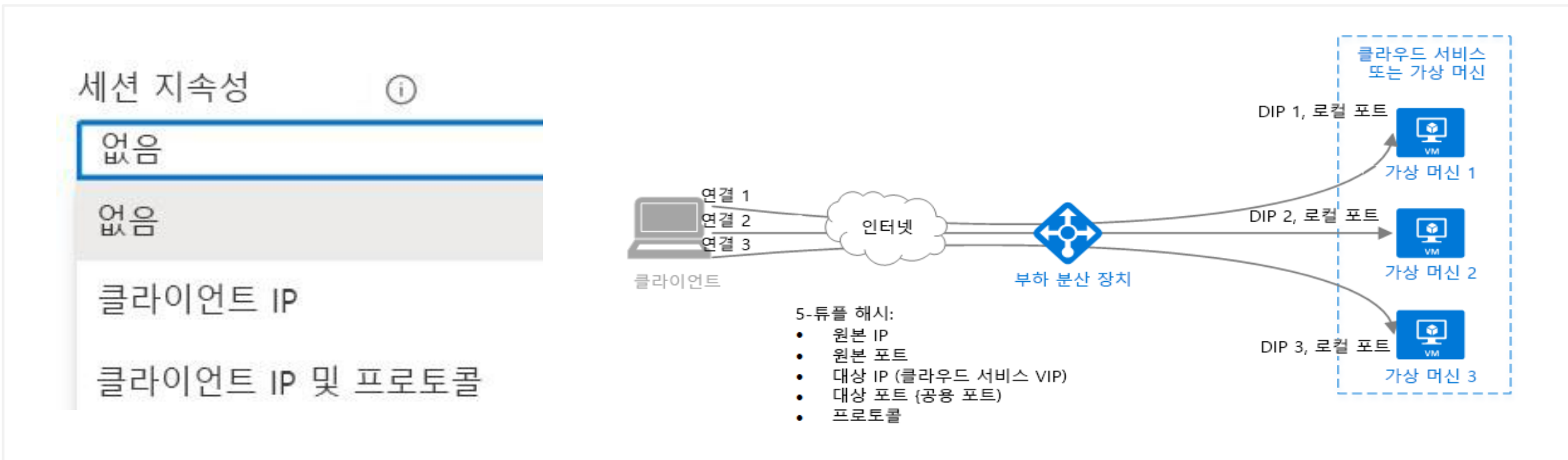
세션 지속성 ①

유류 제한 시간(분) \* ①

TCP 재설정 ☒ 사용 안 함 ☐ 사용

부동 IP ① ☒ 사용 안 함 ☐ 사용

# 세션 지속성 구성(선택 사항)



세션 지속성은 클라이언트 트래픽을 처리하는 방법을 지정합니다.

**없음** (기본) 요청은 모든 가상 머신에서 처리할 수 있습니다.

**클라이언트** IP요청은 동일한 가상 머신에서 처리할 수 있습니다.

**클라이언트 IP 및 프로토콜**은 동일한 주소 및 프로토콜의 연속 요청을 동일한 가상 머신에서 처리하도록 지정합니다.

# 요약 및 리소스 - Azure Load Balancer 구성

지식 점검 문제



Microsoft Learn 모듈([docs.microsoft.com/ko-kr/Learn](https://docs.microsoft.com/ko-kr/Learn))

[Azure Load Balancer를 사용하여 애플리케이션 스케일링  
성능 및 복원력 개선\(샌드박스\)](#)

[Azure에서 비HTTP\(S\) 트래픽 부하 분산](#)

샌드박스는 실습 연습을 나타냅니다.

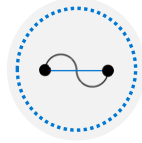
# Azure Application Gateway 구성



# Azure Application Gateway 구성 소개



Application Gateway 구현



Application Gateway 라우팅 결정

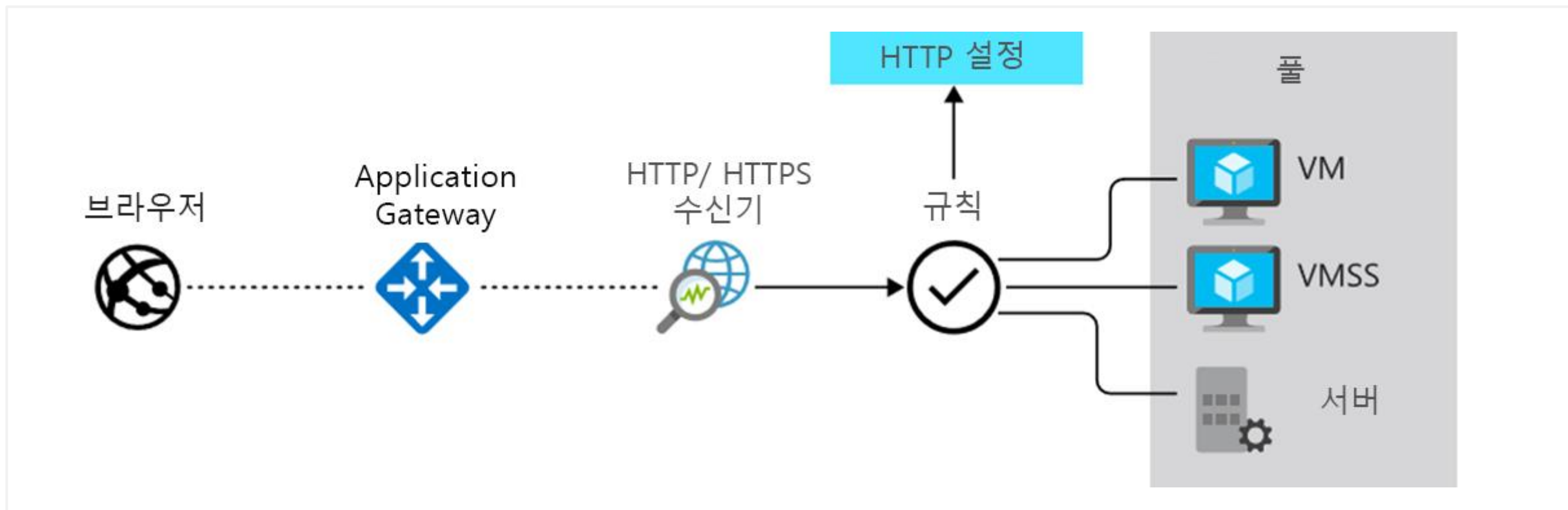


Application Gateway 구성 요소 설정(선택 사항)



요약 및 리소스

# Application Gateway 구현



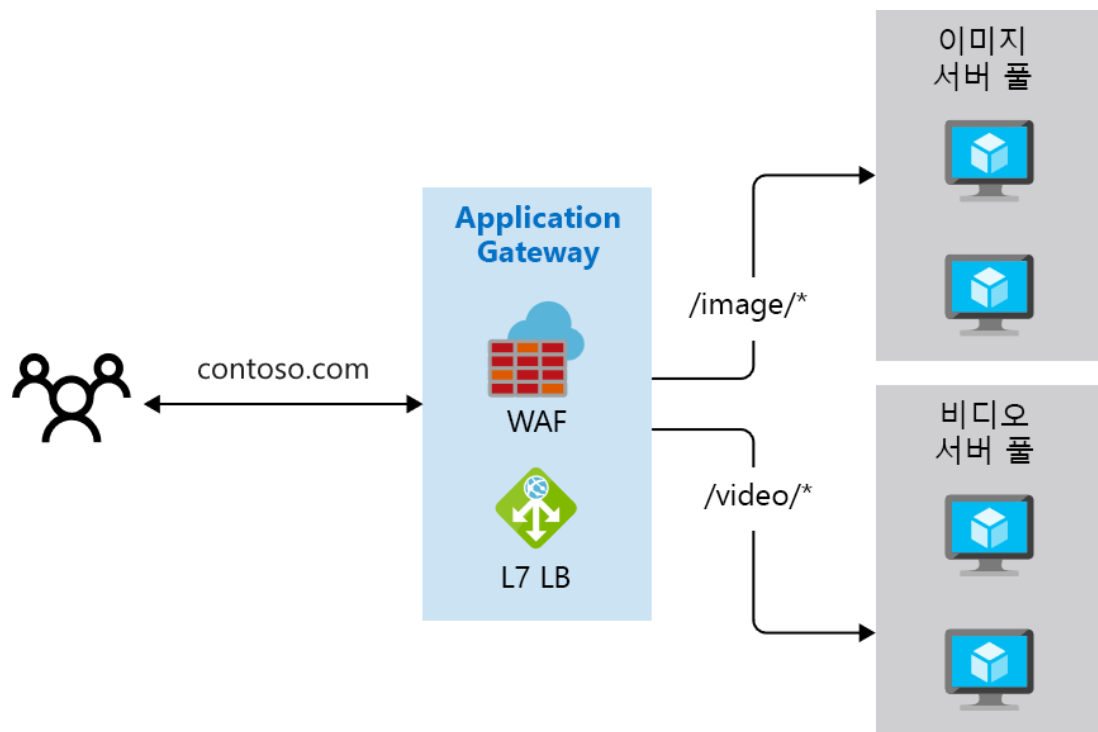
웹  
앱 요청 관리

요청의 URL을 기반으로 트래픽을 웹  
서버 풀로 라우팅합니다.

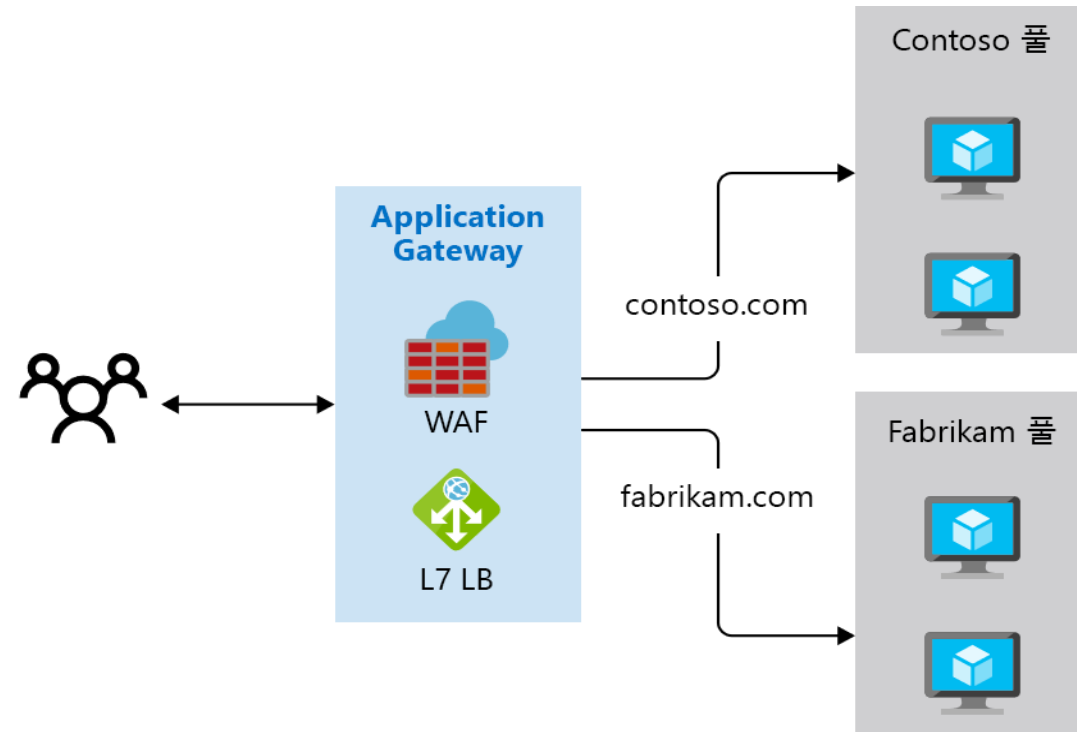
웹 서버는 Azure 가상 머신, Azure 가상  
머신 확장 집합, Azure App Service일 수  
있으며 온-프레미스 서버일  
수도 있습니다.

# Application Gateway 라우팅 결정

## 경로 기반 라우팅



## 다중 사이트 라우팅





# Application Gateway 구성 요소 설정(선택 사항)

프런트 엔드 IP

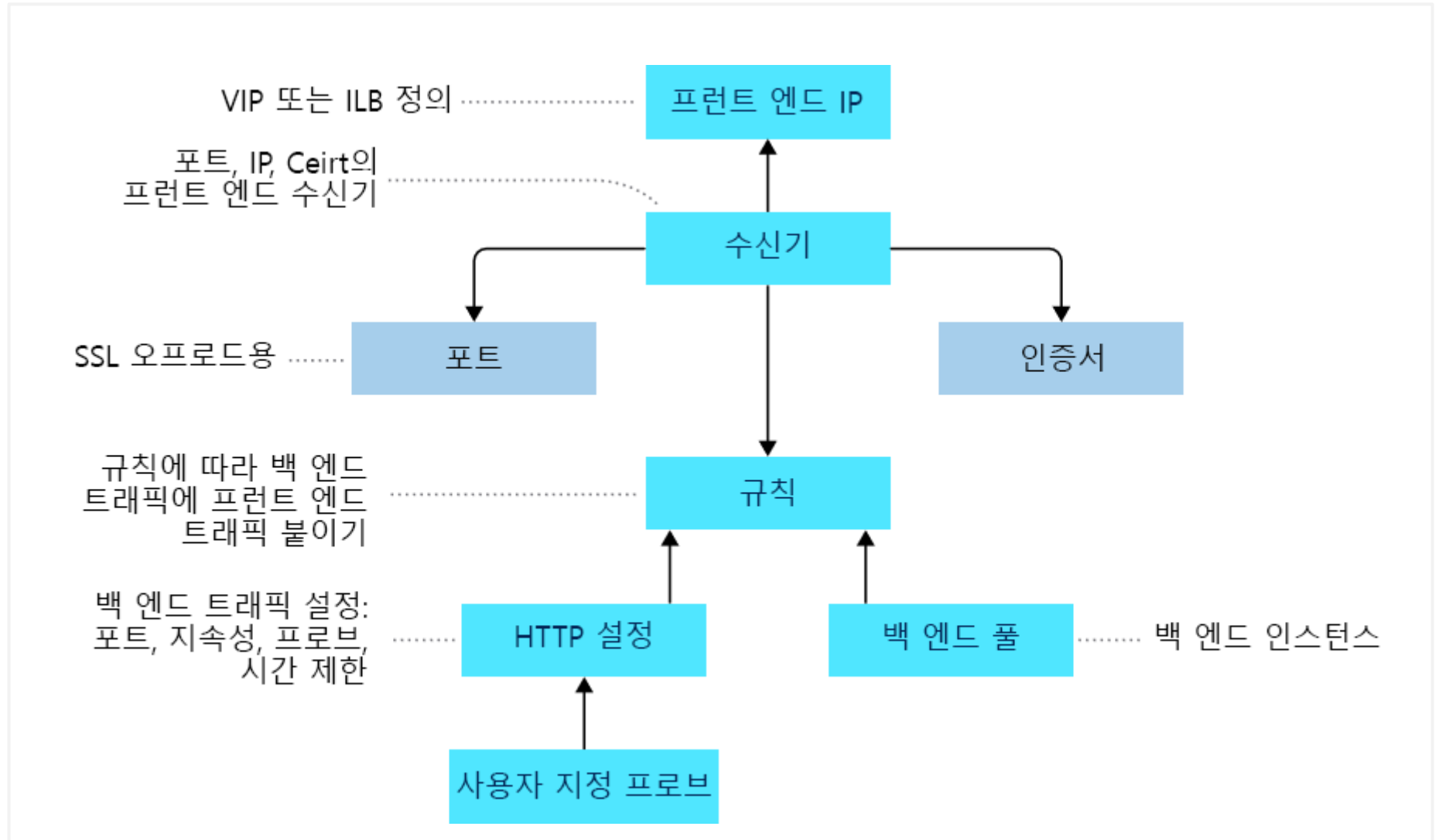
수신기

라우팅 규칙

백 엔드 풀

Web Application Firewall(선택 사항)

상태 프로브



# 요약 및 리소스 - Azure Application Gateway 구성

지식 점검 문제

Microsoft Learn 모듈([docs.microsoft.com/ko-kr/Learn](https://docs.microsoft.com/ko-kr/Learn))



[Azure Application Gateway 소개](#)

[Application Gateway를 사용하여 웹 서비스 트래픽 부하 분산](#)






[Azure에서 HTTP\(S\) 트래픽 부하 분산](#)

[Azure Application Gateway를 사용하여 네트워크 트래픽 엔드투엔드 암호화](#)

# Network Watcher 구성



# Network Watcher 구성 소개

-  Network Watcher 기능 설명
-  IP 흐름 확인 진단 검토
-  다음 홉 진단 검토
-  네트워크 토폴로지 시각화
-  요약 및 리소스

# Network Watcher 기능 설명

**지역 서비스**는 다양한 네트워크 진단 및 모니터링 도구를 제공합니다.

**IP 흐름 확인** 연결 문제 진단

다음 홉은 트래픽이 올바르게 라우팅되어 있는지 여부를 결정합니다.

**VPN** 진단은 게이트웨이 및 연결 문제를 해결합니다.

**NSG** 흐름 로그는 네트워크 보안 그룹을 통해 IP 트래픽을 매핑합니다.

연결 문제 해결은 원본 VM과 대상 간의 연결을 보여 줍니다.




토폴로지가 리소스의 시각적 다이어그램을 생성합니다.

## Network Watcher

### 모니터링

-  토폴로지
-  연결 모니터(클래식)
-  연결 모니터
-  네트워크 성능 모니터

### 로그

-  NSG 흐름 로그
-  진단 로그
-  트래픽 분석

### 네트워크 진단 도구

-  IP 흐름 확인
-  NSG 진단
-  다음 홉
-  유효한 보안 규칙
-  VPN 문제 해결
-  패킷 캡처
-  연결 문제 해결

# IP 흐름 확인 진단 검토

IP 흐름 확인은 가상 머신 간 패킷이 허용 또는 거부되는지를 확인합니다.

모니터링

토폴로지

연결 모니터(클래식)

연결 모니터

네트워크 성능 모니터

네트워크 진단 도구

IP 흐름 확인

NSG 진단

다음 홈

유효한 보안 규칙

VPN 문제 해결

패킷 캡처

연결 문제 해결

패킷 세부 정보

프로토콜  
☒ TCP ☐ UDP

방향  
☒ 인바운드 ☐ 아웃바운드

로컬 IP 주소 \* ⓘ  
10.1.1.4 ✓

로컬 포트 \* ⓘ  
3389 ✓

원격 IP 주소 \* ⓘ  
13.24.35.46 ✓

원격 포트 \* ⓘ  
3389 ✓

선택

접근 불가

보안 규칙  
DenyAllInBound

# 다음 홉 진단 검토

다음 홉을 표시하여 트래픽이 올바른 대상으로 전송되는지 여부를 쉽게 확인할 수 있습니다.

구독 \* ⓘ

MSDN Platforms Subscription

리소스 그룹 \* ⓘ

Demo

가상 머신 \* ⓘ

vm01

네트워크 인터페이스 \*

vm01165

원본 IP 주소 \* ⓘ

10.1.1.4

대상 IP 주소 \* ⓘ

13.24.35.46

다음 홉

결과


다음 홉 유형

없음

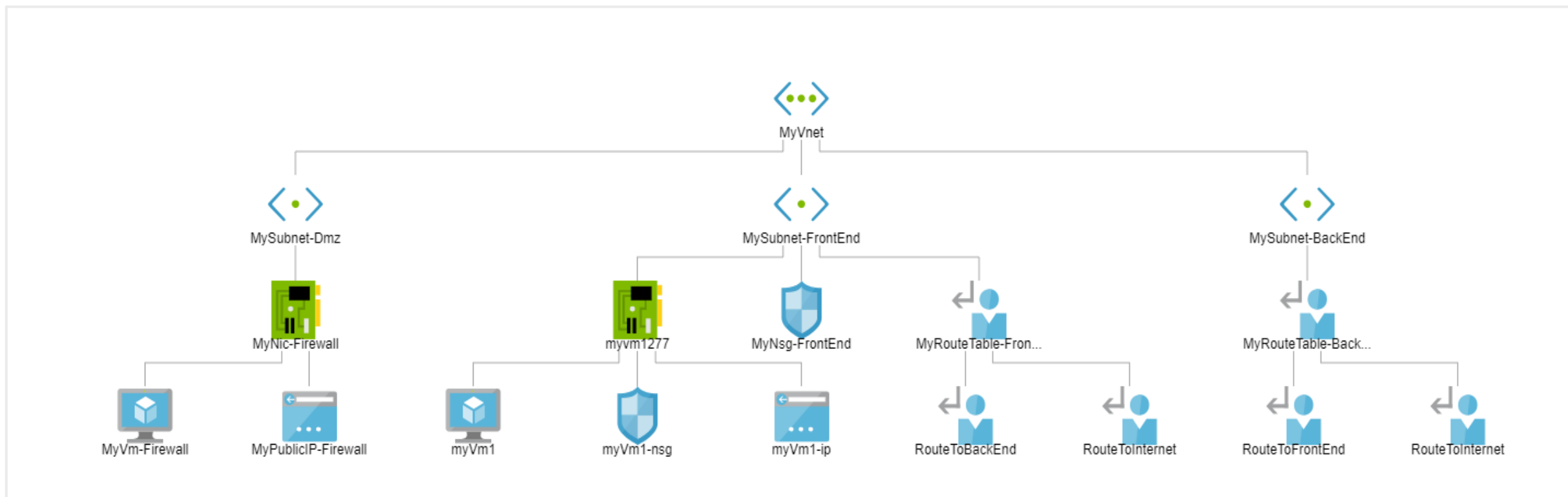
IP 주소

10.1.1.100

우팅 테이블 ID

/subscriptions/2301e3a0-8420-... 

# 네트워크 토폴로지 시각화



네트워킹 요소의 시각적  
표현 제공

가상 네트워크의 모든 리소스,  
리소스 간 연결, 리소스 간 관계를  
확인할 수 있습니다.

Network Watcher  
인스턴스는 가상 네트워크와  
동일한 지역에 있습니다.



# 요약 및 리소스 - Network Watcher 구성

지식 점검 문제



Microsoft Learn 모듈([docs.microsoft.com/ko-kr/Learn](https://docs.microsoft.com/ko-kr/Learn))

[Azure Network Watcher 소개](#)

[네트워크 모니터링 도구를 사용하여 엔드투엔드 Azure  
네트워크 인프라 모니터링 및 문제 해결](#)

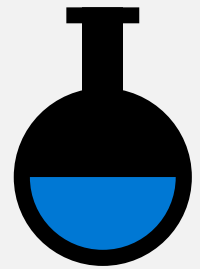
[Azure Monitor 로그를 사용하여 Azure 인프라  
분석\(샌드박스\)](#)

[Azure Monitor VM Insights를 사용하여 가상 머신의  
성능 모니터링\(샌드박스\)](#)

[Kusto Query Language를 사용하여 첫 번째 쿼리 작성](#)

샌드박스는 실습 연습을 나타냅니다.

# 랩: 트래픽 관리 구현



# 랩 06 - 트래픽 관리 구현

## 시나리오

네트워크 트래픽에 대한 허브 스포크 토폴로지 구현을 담당합니다. 토폴로지에는 Azure Load Balancer 및 Azure Application Gateway가 포함되어야 합니다.

## 목표

### 작업 1:

랩 환경 프로비저닝

### 작업 2:

허브 및 스포크 네트워크  
토폴로지 구성

### 작업 3:

가상 네트워크 피어링의  
전이성 테스트

### 작업 4:

허브 및 스포크 토폴로지에서  
라우팅 구성

### 작업 5:

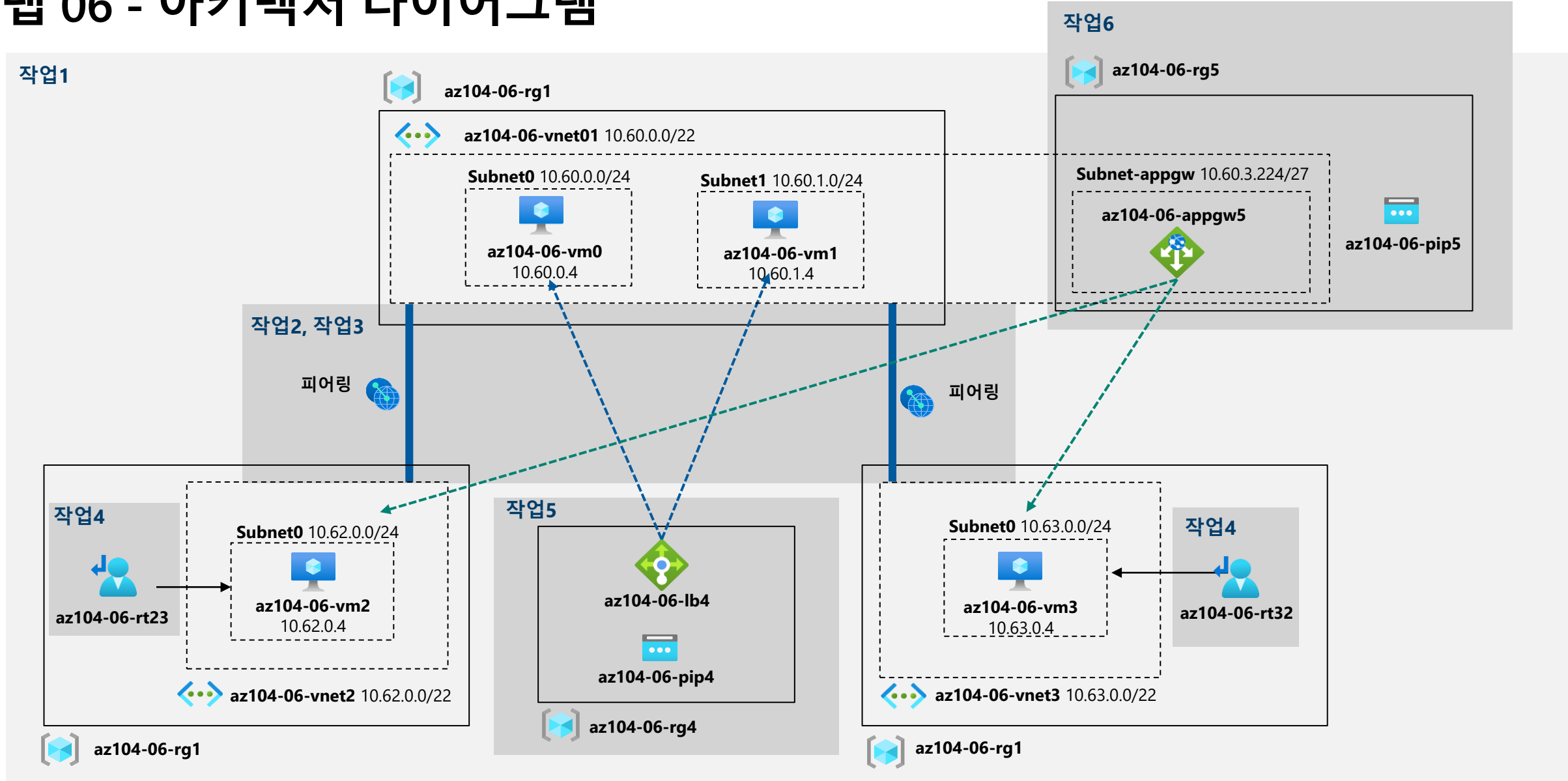
Azure Load Balancer  
구현

### 작업 6:

Azure Application Gateway  
구현

다음 슬라이드에서 아키텍처 다이어그램을 확인할 수 있습니다. ➔

# 랩 06 - 아키텍처 다이어그램



프레젠테이션 종료

