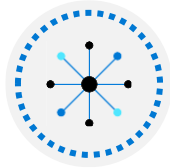


AZ-104T00A

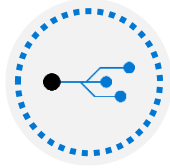
가상 네트워킹 관리



가상 네트워킹 관리 소개



Virtual Networks 구성



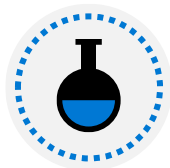
네트워크 보안 그룹 구성



Azure Firewall 구성



Azure DNS 구성

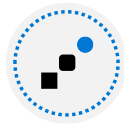


랩 04 - 가상 네트워크 구현

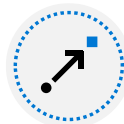
Virtual Networks 구성



가상 네트워킹 구성 소개



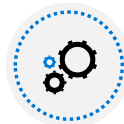
가상 네트워크 계획



서브넷 만들기



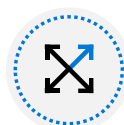
가상 네트워크 만들기



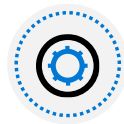
IP 주소 지정 계획



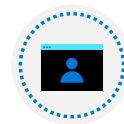
공용 IP 주소 만들기



공용 IP 주소 연결



개인 IP 주소 연결

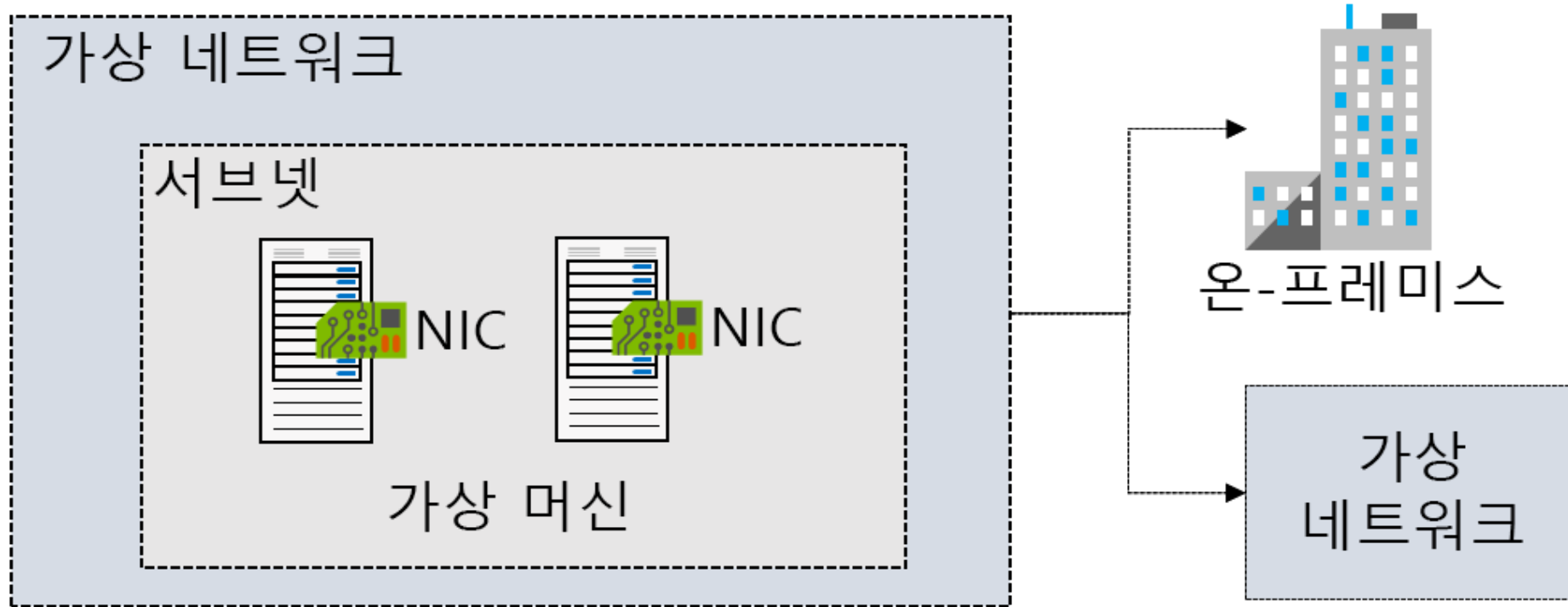


데모 - 가상 네트워크



요약 및 리소스

가상 네트워크 계획



네트워크의
논리적 표현

프라이빗 클라우드
전용 가상 네트워크
만들기

가상 네트워크를
사용하여 안전하게
데이터 센터 확장

하이브리드 클라우드
시나리오 활성화

Azure 가상 네트워크의 기능

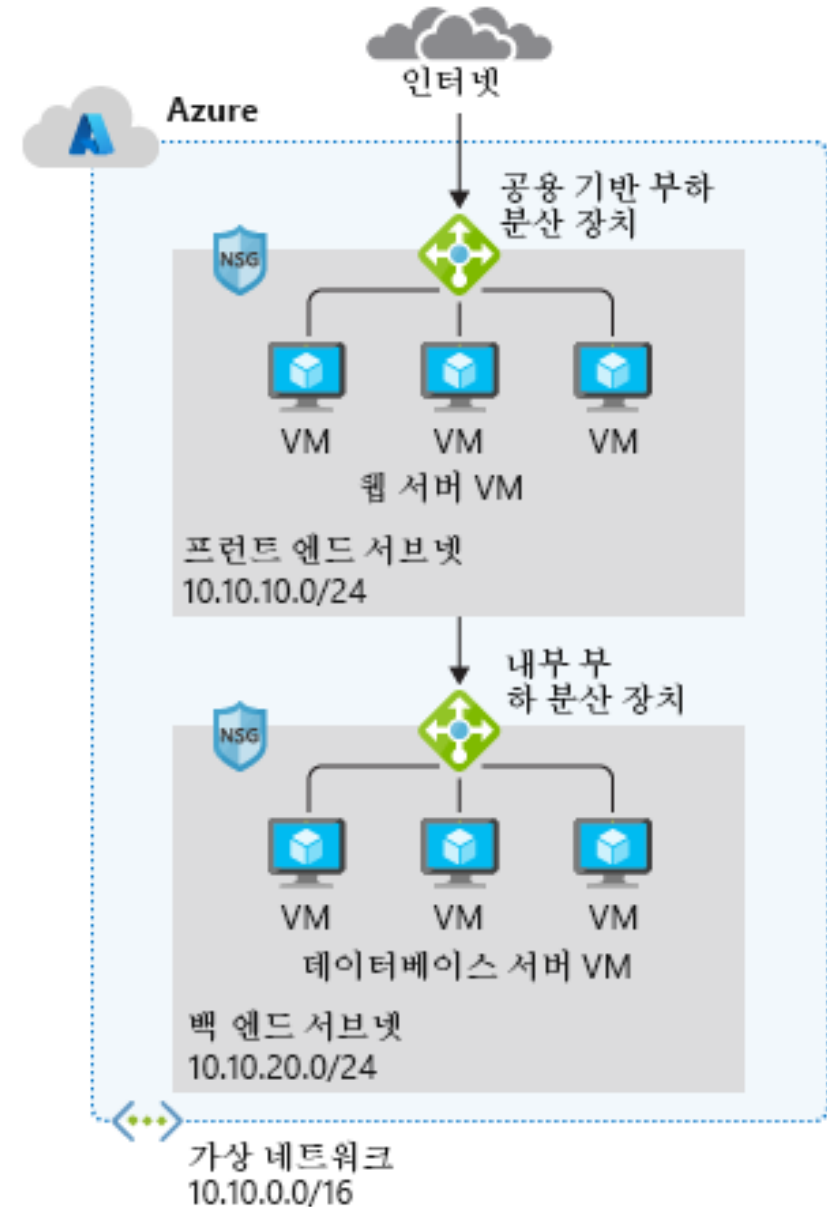
인터넷과의 통신

Azure 리소스 간 통신

온-프레미스 리소스와의 통신

네트워크 트래픽 필터링

네트워크 트래픽 라우팅



가상 네트워크 주소 공간

RFC 1918

10.0.0.0 - 10.255.255.255(10/8 접두사)

172.16.0.0 - 172.31.255.255(172.16/12 접두사)

192.168.0.0 - 192.168.255.255(192.168/16 접두사)

Azure에서 예약되는 5개 IP 주소

- x.x.x.0: 네트워크 주소
- x.x.x.1: 기본 게이트웨이로 Azure에서 예약됨
- x.x.x.2, x.x.x.3: Azure DNS IP를 VNet 공간에 매핑하기 위해 Azure에서 예약됨
- x.x.x.255: 네트워크 브로드캐스트 주소

사용할 수 없는 주소 범위:

- 224.0.0.0/4(멀티캐스트)
- 255.255.255.255/32(브로드캐스트)
- 127.0.0.0/8(루프백)
- 169.254.0.0/16(링크-로컬)
- 168.63.129.16/32(내부 DNS)

네트워크의 논리적
표현

프라이빗 클라우드만
사용하는 전용 가상 네
트워크 만들기

가상 네트워크를 사용
하여안전하게 데이터
센터 확장

하이브리드
클라우드 시나리오
사용

서브넷 만들기

+ 서브넷 + 게이트웨이 서브넷 새로 고침 사용자 관리 삭제				
이름 ↑↓	IPv4 ↑↓	IPv6 ↑↓	사용 가능한 IP ↑↓	위임 대상
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/27	-	27	-
GatewaySubnet	10.0.3.0/27	-	동적 사용에 따른 가용성	-

가상 네트워크는 하나 이상의 서브넷으로 분할될 수 있습니다.

서브넷은 네트워크의 논리적 구분을 지원합니다.

서브넷을 사용하면 보안/성능을 개선하고 네트워크를 더 쉽게 관리할 수 있습니다.

각 서브넷에는 고유한 주소 범위가 있어야 합니다. 즉, 구독의 vnet에 포함된 다른 서브넷과 주소 범위가 겹쳐서는 안 됩니다.

가상 네트워크 만들기

언제든 새 가상 네트워크를 만듭니다.

가상 머신을 만들 때 가상 네트워크를 추가합니다.

주소 공간과 서브넷 하나 이상을 정의해야 합니다.

주소 공간이 겹치지 않도록 주의합니다.

가상 네트워크 만들기

기본 사항 IP 주소 보안 태그 검토 + 만들기

프로젝트 정보

구독 * ⓘ

Visual Studio Enterprise

리소스 그룹 * ⓘ

Lab04

[새로 만들기](#)

인스턴스 정보

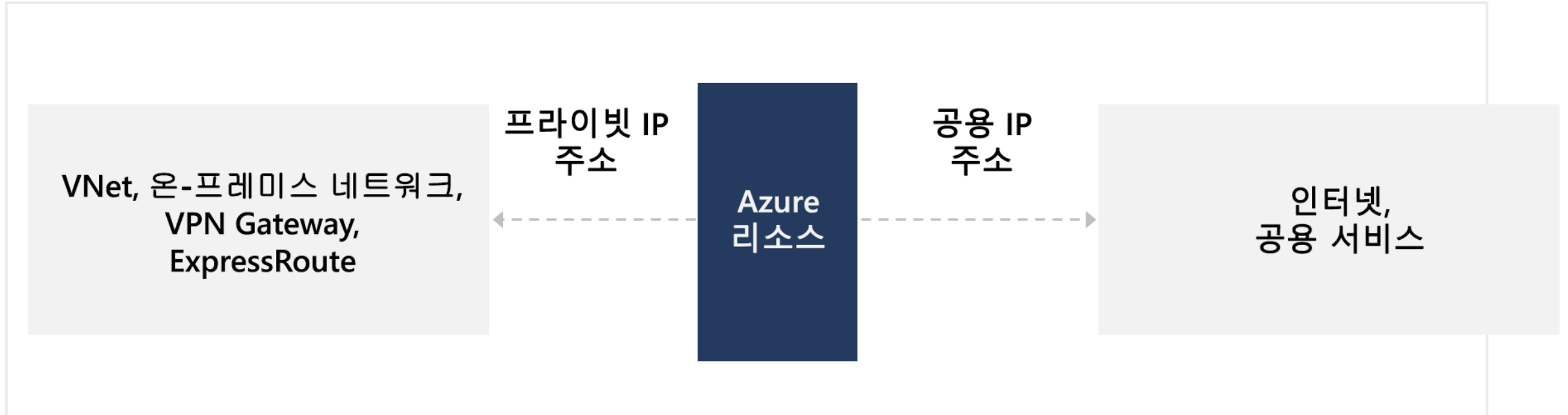
이름 *

VNet2

지역 *

(US) 미국 동부 2

IP 주소 지정 계획



개인 IP 주소 - VPN 게이트웨이 또는 ExpressRoute 회로를 사용하여 네트워크를 Azure로 확장할 때 Azure VNet(Virtual Network) 및 온-프레미스 네트워크 내에서 사용됩니다.

공용 IP 주소 - Azure 공용 서비스를 비롯한 인터넷과의 통신에 사용됩니다.

개인 IP 주소 할당

개인 IP 주소	IP 주소 연결
Virtual Machine	NIC
내부 부하 분산 장치	프런트 엔드 구성
Application Gateway	프런트 엔드 구성

동적(기본값). Azure는 사용 가능한 다음 할당되지 않은 또는 예약되지 않은 IP 주소를 서브넷의 주소 범위에 할당합니다.

Static. 서브넷의 주소 범위에서 모든 할당되지 않은 또는 예약되지 않은 IP 주소를 선택하여 할당합니다.

공용 IP 주소 만들기

IPv4 또는 IPv6 또는 둘 다에서 사용 가능

기본 대 표준 SKU

동적 및 고정

영역 중복(표준 SKU)

접두사로 사용할 수 있는 인접 주소 범위

공용 IP 주소 만들기

IP 버전 *

IPv4

IPv6

Both

SKU *

기본

표준

IPv4 IP 주소 구성

이름 *

IP 주소 할당 *

동적

정적

© Copyright Microsoft Corporation. All rights reserved.

공용 IP에 적합한 SKU 선택

기본 SKU

- 고정 또는 동적 할당 방법으로 할당됩니다.
- 기본적으로 엽니다. 필요에 따라 NSG를 사용하는 것이 좋습니다.
- 네트워크 인터페이스 또는 VPN Gateway, 공용 부하 분산 장치, Application Gateway에 할당됩니다.
- 가용성 영역 시나리오를 지원하지 않습니다.

표준 SKU

- 항상 고정 할당 방법을 사용합니다.
- 기본적으로 보호되며 닫혀 있으므로 인바운드 트래픽을 수신하지 않습니다.
- NSG를 사용하여 인바운드 트래픽을 허용합니다.
- 네트워크 인터페이스, 표준 공용 부하 분산 장치 또는 Application Gateway에 할당됩니다.
- 영역 중복 SKU이거나 영역 SKU일 수도 있고 영역이 없는 SKU일 수도 있습니다.

공용 IP 주소

공용 IP 주소	IP 주소 연결	동적	정적
Virtual Machine	NIC	예	예
Load Balancer	프런트 엔드 구성	예	예
VPN Gateway	게이트웨이 IP 구성	예(비 AZ만 해당)	예
Application Gateway	프런트 엔드 구성	예(V1에만 해당)	예(V2에만 해당)
Azure Firewall	프런트 엔드 구성	아니요	예
NAT 게이트웨이	게이트웨이 IP 구성	아니요	예

공용 IP 주소 리소스는 가상 머신 네트워크 인터페이스, 인터넷 연결 부하 분산 장치, VPN Gateway, 애플리케이션 게이트웨이와 같은 리소스와 연결할 수 있습니다.

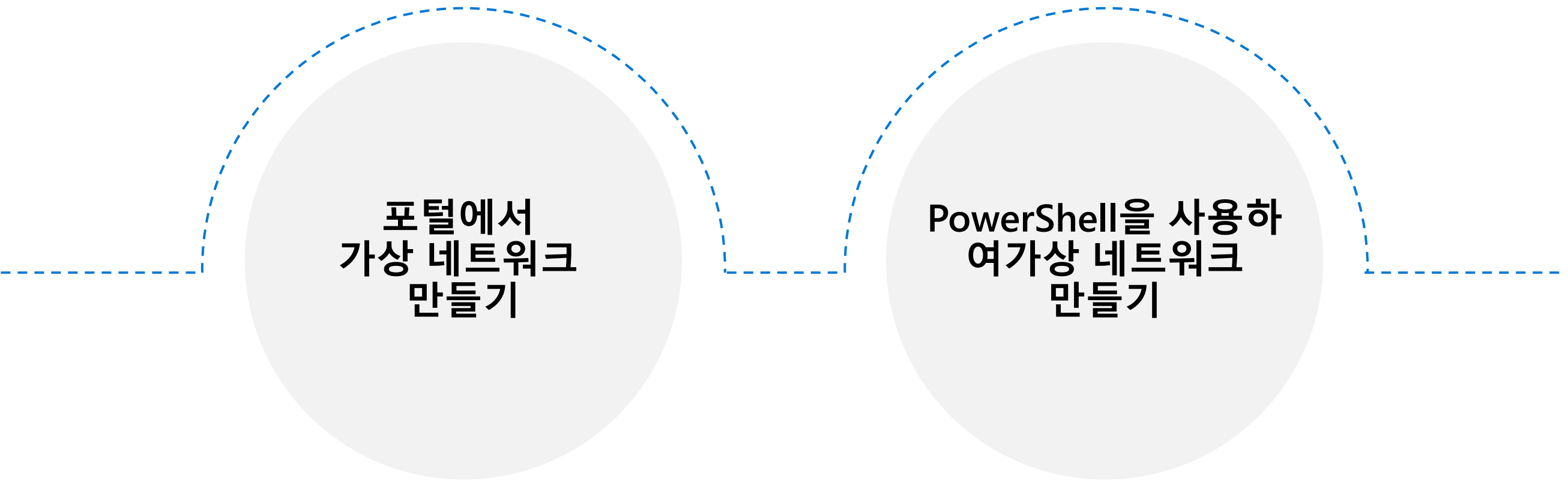
개인 IP 주소 연결

개인 IP 주소	IP 주소 연결	동적	정적
가상 머신	NIC	예	예
내부 부하 분산 장치	프런트 엔드 구성	예	예
Application Gateway	프런트 엔드 구성	예	예

동적(기본값). Azure가 서브넷의 주소 범위에서 사용 가능한 다음 미할당/미예약 IP 주소를 할당합니다.

정적. 서브넷의 주소 범위에서 모든 미할당/미예약 IP 주소를 선택하여 할당합니다.

데모 - 가상 네트워크



The diagram consists of two light gray circles connected by a dashed blue line. Each circle contains text describing a method for creating a virtual network. The left circle is labeled '포털에서 가상 네트워크 만들기' (Create virtual network from portal) and the right circle is labeled 'PowerShell을 사용하여 가상 네트워크 만들기' (Create virtual network using PowerShell). The dashed blue line starts on the left, goes up and over the first circle, then down and over the second circle, and finally goes up and over the third circle.

포털에서
가상 네트워크
만들기

PowerShell을 사용하
여 가상 네트워크
만들기

요약 및 리소스 - 가상 네트워크 구성

지식 점검



Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)

[Azure 배포에 대한 IP 주소 지정 스키마 디자인\(샌드박스\)](#)

[Windows Server IaaS VM IP 주소 지정 및 라우팅 구현](#)

샌드박스는 실습 연습을 나타냅니다.

네트워크 보안 그룹 구성



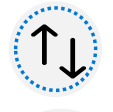
네트워크 보안 그룹 구성 소개



NSG(네트워크 보안 그룹) 구현



NSG 규칙 확인



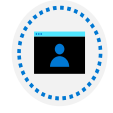
NSG 유효 규칙 확인



NSG 규칙 만들기



ASG(애플리케이션 보안 그룹) 구현



데모 - NSG



요약 및 리소스

NSG(네트워크 보안 그룹) 구현

The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'nsg0'. The left sidebar contains navigation links: '개요' (Overview), '활동 로그' (Activity Log), '액세스 제어(IAM)' (Access Control (IAM)), '태그' (Tags), and '문제 진단 및 해결' (Troubleshooting and support). The main content area is titled '기본 정보' (Basic information) and lists the following details:

- 리소스 그룹 (변경): rg01
- 위치: 미국 동부
- 구독 (변경): Azure Pass - Sponsorship
- 구독 ID:
- 태그 (변경): [태그를 추가하려면 여기를 클릭](#)

On the right side, additional information is provided:

- 사용자 지정 보안 규칙: 1 인바운드, 0 아웃바운드
- 연결된 대상: 1개 서브넷, 0개 네트워크 인터페이스

네트워크 트래픽을 한
가상 네트워크의
리소스로 제한합니다.

인바운드 또는
아웃바운드 네트워크
트래픽을 허용 또는
거부하는 보안 규칙을
나열합니다.

서브넷 또는
네트워크인터페이
스에 연결됩니다.

여러 번 연결할
수 있습니다.

NSG 규칙 확인

인바운드 보안 규칙						
우선 순위	이름	포트	프로토콜	소스	대상 주소	작업
300	⚠ RDP	3389	TCP	모두	모두	✔ 허용
65000	AllowVnetInBound	모두	모두	VirtualNetwork	VirtualNetwork	✔ 허용
65001	AllowAzureLoadBalancerInBound	모두	모두	AzureLoadBalancer	모두	✔ 허용
65500	DenyAllInBound	모두	모두	모두	모두	✖ 거부
아웃바운드 보안 규칙						
우선 순위	이름	포트	프로토콜	소스	대상 주소	작업
65000	AllowVnetOutBound	모두	모두	VirtualNetwork	VirtualNetwork	✔ 허용
65001	AllowInternetOutBound	모두	모두	모두	Internet	✔ 허용
65500	DenyAllOutBound	모두	모두	모두	모두	✖ 거부

NSG의 보안 규칙을 사용하면
가상 네트워크 서브넷과 네트워크
인터페이스로 유입/유출될 수 있는
네트워크 트래픽을 필터링할 수 있습니다.

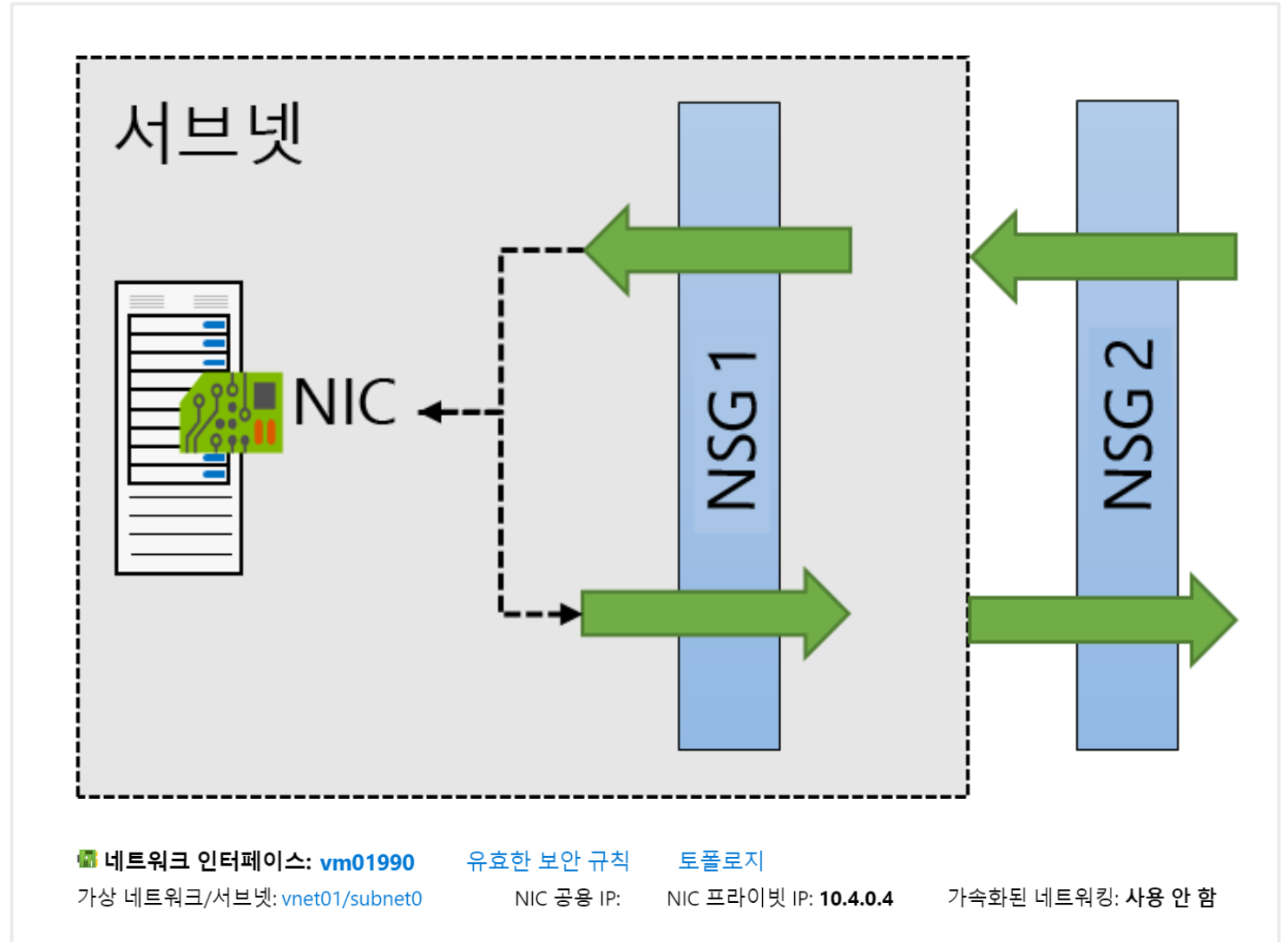
기본 보안 규칙이 있습니다.
기본 규칙을 삭제할 수는 없지만
우선 순위가 높은 다른 규칙을
추가할 수 있습니다

NSG 유효 규칙 확인

NSG는 서브넷과 NIC에 대해 독립적으로 평가됩니다.

트래픽이 허용되려면 두 수준 모두에 "허용" 규칙이 있어야 합니다.

적용되는 보안 규칙이 무엇인지 모르는 경우 유효한 규칙 링크를 사용합니다.




NSG 규칙 만들기

원본(모두, IP 주소, 서비스 태그, 애플리케이션 보안 그룹)

대상(모두, IP 주소, 가상 네트워크, 애플리케이션 보안 그룹)

서비스(HTTPS, SSH, RDP, DNS, POP3, 사용자 지정 등)

우선 순위 – 숫자가 낮을수록 우선 순위가 높음

 **인바운드 보안 규칙 추가**
NW-APP01NSG

소스 ⓘ
Any ▼

원본 포트 범위 * ⓘ
*

대상 주소 ⓘ
Any ▼

서비스 ⓘ
Custom ▼

대상 포트 범위 * ⓘ
8080

프로토콜
☒ Any ☐ TCP ☐ UDP ☐ ICMP

작업
☒ 허용
☐ 거부

우선 순위 * ⓘ
330 ✓

이름 *

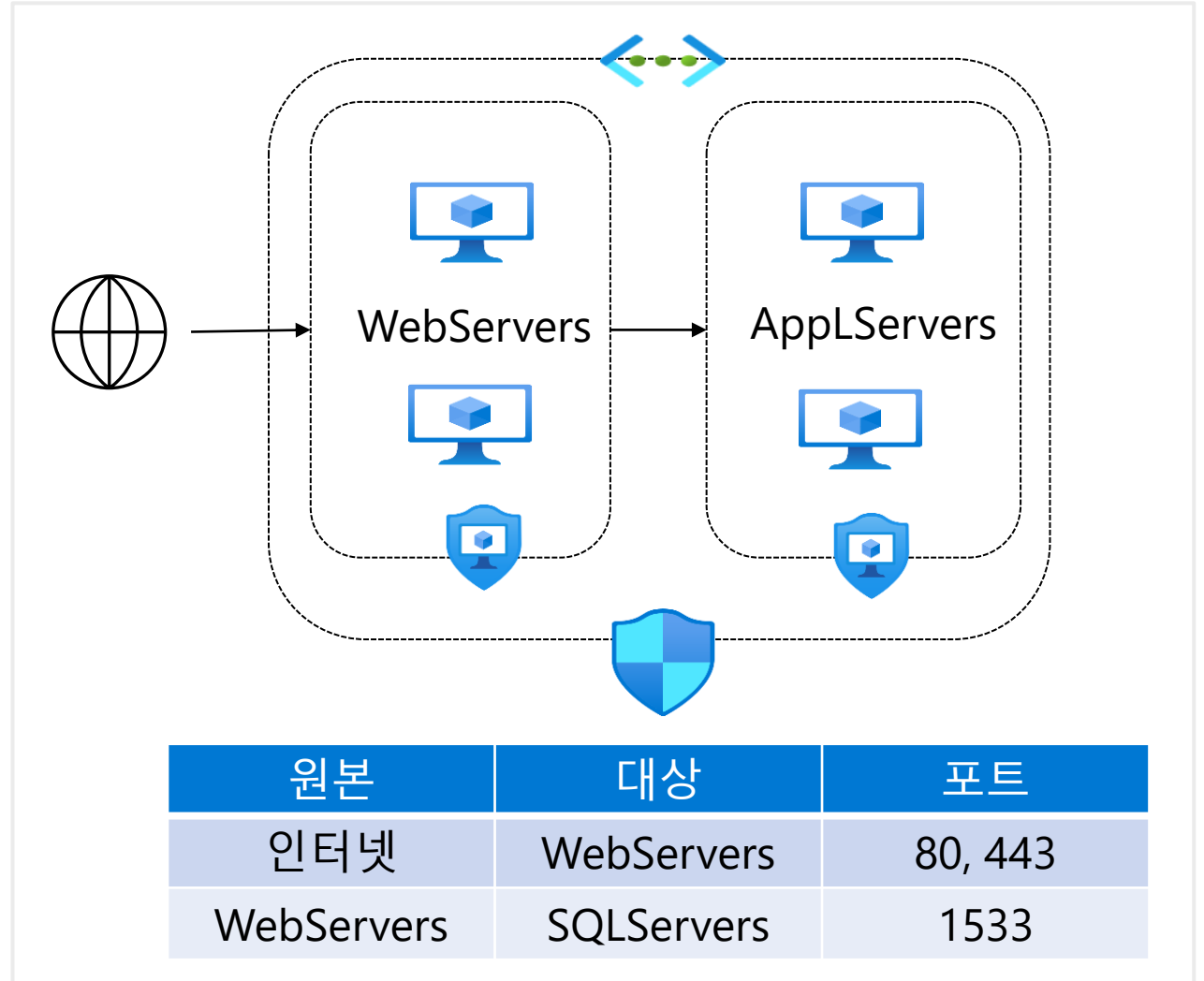
애플리케이션 보안 그룹 구현

애플리케이션 구조 확장

ASG는 논리적으로 웹 서버, 애플리케이션 서버와 같은 가상 머신을 그룹화합니다

트래픽 흐름을 컨트롤하는 규칙 정의

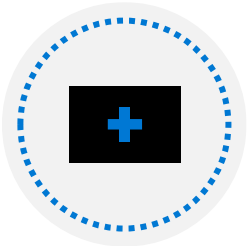
추가 보안을 위해 ASG를 NSG로 래핑합니다



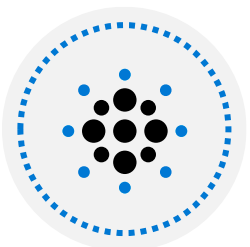
데모 - 네트워크 보안 그룹



NSG 블레이드에 액세스



새 NSG 추가



인바운드 및 아웃바운드 규칙 살펴보기

요약 및 리소스 - 네트워크 보안 그룹 구성

지식 점검



Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)

네트워크 보안 그룹 및 서비스 엔드포인트를 사용하여
Azure 리소스에 대한 액세스 보호 및 격리(샌드박스)

샌드박스는 실습 연습을 나타냅니다.

단원 03: Azure Firewall 구성



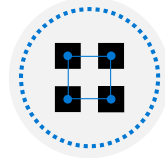
Azure Firewall 구성 소개



Azure Firewall 사용 확인



Azure Firewall 만들기



Azure Firewall 규칙 만들기



요약 및 리소스

Azure Firewall 사용 확인

서비스형 상태 저장 방화벽

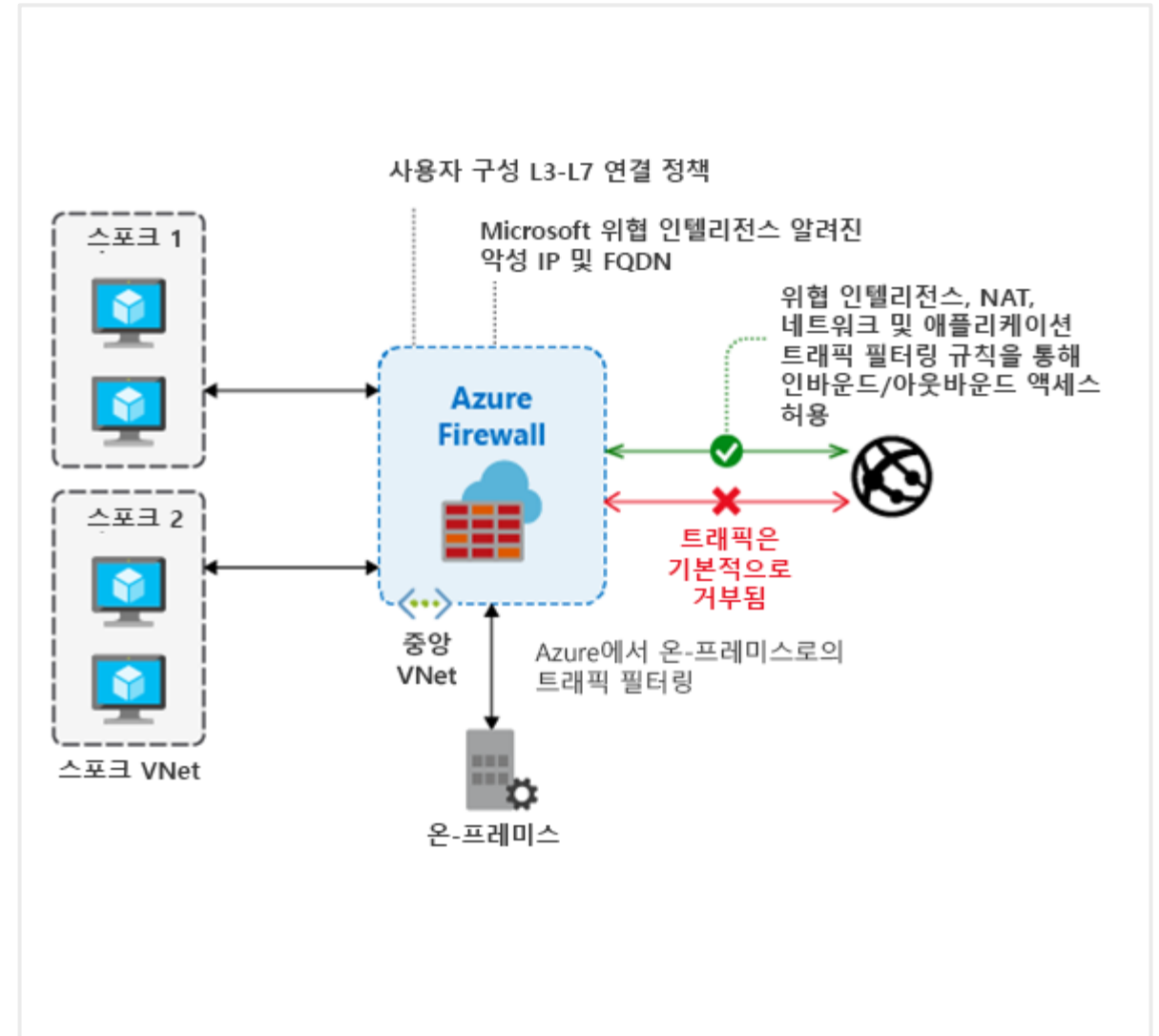
클라우드 확장성의 제한이 없는 기본 제공 고가용성

애플리케이션 및 네트워크 연결 정책 만들기,
적용, 로그

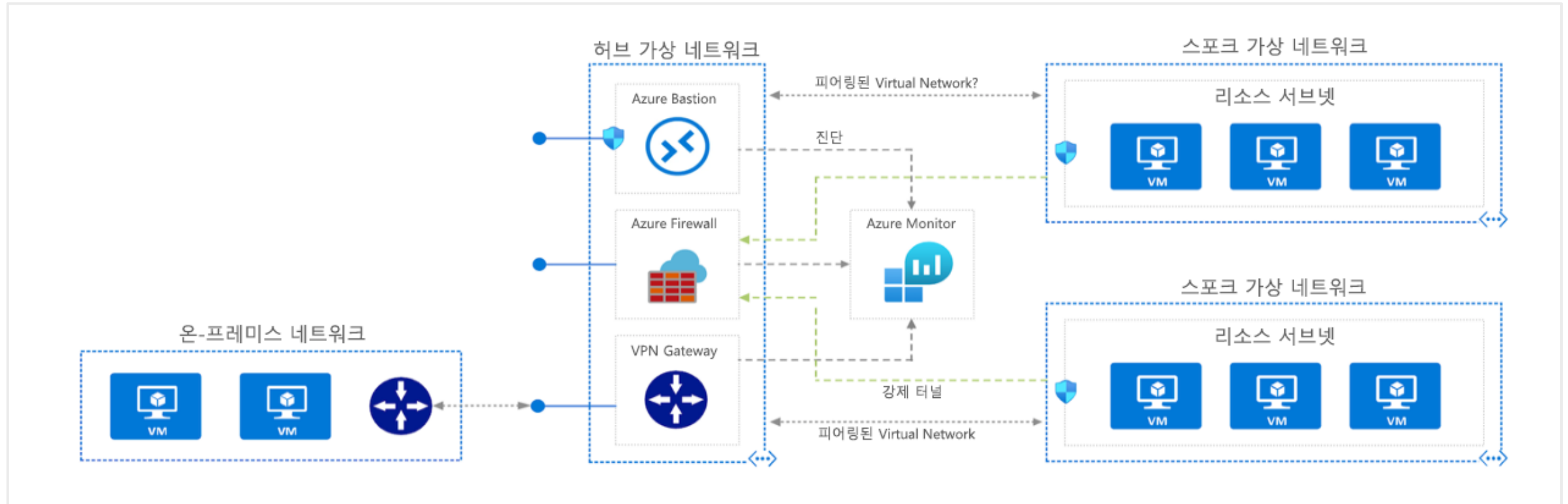
위협 인텔리전스 기반 필터링

로그 및 분석을 위한 Azure Monitor와의 완전한 통합

VPN 및 ExpressRoute 게이트웨이 뒤로 배포하여
하이브리드 연결 지원



Azure Firewall 만들기



허브-스포크 네트워크
토폴로지를 사용하는
것이 좋습니다.

공유 서비스는 허브 가상
네트워크에 배치됩니다.

각각의 환경은 격리 상태를
유지하기 위해 스포크에
배치됩니다.

Azure Firewall 규칙 만들기

Azure Firewall Manager를 사용하면 중앙 집중식으로 방화벽을 관리할 수 있음

방화벽 정책 컨테이너 규칙과 설정을 통해 액세스 제어

NAT 규칙은 들어오는 연결을 허용함

네트워크 규칙에는 원본과 대상 주소, 프로토콜, 대상 포트가 포함됨

애플리케이션 규칙은 서브넷에서 액세스할 수 있는 FQDN(정규화된 도메인 이름)을 **제공**함

홈 > ContosoFirewallPolicy



ConFirewallPolicy

방화벽 정책

설정



부모 정책



규칙 컬렉션



DNAT 규칙



네트워크 규칙



응용 프로그램 규칙



DNS

요약 및 리소스 - Azure Firewall

지식 점검

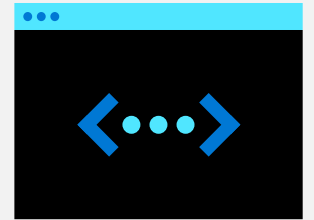


Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)

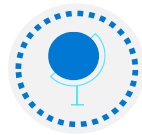
[Azure Firewall 소개](#)

[Azure Firewall Manager 소개](#)

Azure DNS 구성.



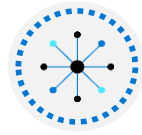
Azure DNS 구성 소개



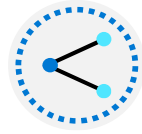
도메인 및 사용자 지정 도메인 식별



사용자 지정 도메인 이름 확인(선택 사항)



Azure DNS 영역 만들기



DNS 도메인 위임



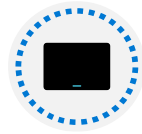
DNS 레코드 집합 추가



프라이빗 DNS 영역에 대한 계획



프라이빗 영역 시나리오 확인



데모 – DNS 이름 확인



요약 및 리소스

도메인 및 사용자 지정 도메인 식별

Azure 구독을 만들 때 Azure AD 도메인이 만들어집니다.

초기 도메인 이름의 양식은
*domainname.onmicrosoft.com*입니다.

이름을 사용자 지정/변경할 수 있습니다.

사용자 지정 이름은 추가한 후에 반드시
확인해야 합니다. 그래야 도메인 소유권을
증명할 수 있습니다.

디렉터리 만들기
Azure Active Directory

기본 * 구성 * 검토 + 만들기

디렉터리 세부 정보
새 디렉터리 구성

조직 이름 * ⓘ
Azure Administrator Incorporated

초기 도메인 이름 * ⓘ
azureadminincorg
.onmicrosoft.com

국가/지역 ⓘ
미국

✓ 데이터 센터 위치 - 미국
데이터 센터 위치는 위에서 선택한 국가/지역에 따라 결정됩니다.

검토 + 만들기 < 이전 다음: 검토 + 만들기 >



사용자 지정 도메인 이름
Contoso

사용자 지정 도메인 이름 * ⓘ
azureadmininc.org ✓

도메인 추가

Azure DNS 영역 만들기

DNS 영역은 도메인에 대한 DNS 레코드를 호스트합니다.

여러 영역이 동일한 이름을 공유하는 경우 각 인스턴스에 다른 이름 서버 주소가 할당됩니다.

루트/상위 도메인은 등록 기관에 등록되어 Azure NS를 가리킵니다.

DNS 영역 만들기

기본 사항

태그

검토 + 만들기

DNS 영역은 특정 도메인의 DNS 레코드를 호스트하는 데 사용됩니다. 예를 들어, 'contoso.com'이라는 도메인은 'mail.contoso.com'(메일 서버)과 'www.contoso.com'(웹 사이트) 같은 여러 개의 DNS 레코드를 포함할 수 있습니다. Azure DNS를 통해 DNS 영역을 호스트하고, DNS 레코드를 관리하며, 사용자가 만든 DNS 레코드를 사용하는 최종 사용자의 DNS 쿼리에 응답하는 이름 서버를 제공할 수 있습니다. [자세한 정보](#)

프로젝트 정보

구독 *

리소스 그룹 *

이름 *

리소스 그룹 위치 ①

MSDN Platforms Subscription

azureadmininc.org

rg-dns

(US) 미국 동부 2

새로 만들기

검토 + 만들기

이전

다음: 태그 >

자동화에 대한 템플릿 다운로드

DNS 도메인 위임

Azure DNS에 도메인을 위임할 때는 Azure DNS에서 제공하는 4개의 이름 서버 이름을 모두 사용해야 합니다.

DNS 영역이 만들어지면 부모 등록 기관을 업데이트합니다.

자식 영역의 경우 부모 도메인에 NS 레코드를 등록합니다.

 **azureadmininc.org**
DNS 영역

[+ 레코드 집합](#) [→ 이동](#) [🗑️ 영역 삭제](#) [🔄 새로 고침](#)

리소스 그룹 ([변경](#))
[rg-dns](#)

구독 ([변경](#))
[MSDN Platforms Subscription](#)

구독 ID

이름 서버 1
ns1-03.azure-dns.com.

이름 서버 2
ns2-03.azure-dns.net.

이름 서버 3
ns3-03.azure-dns.org.

이름 서버 4
ns4-03.azure-dns.info.

태그 ([변경](#))
[태그를 추가하려면 여기를 클릭](#)

DNS 레코드 집합 추가

레코드 집합은 이름과 유형이 같은 영역의 레코드 컬렉션입니다.

모든 레코드 집합에는 최대 20개의 레코드를 추가할 수 있습니다.

레코드 집합에는 두 개의 동일한 레코드가 포함될 수 없습니다.

드롭다운 유형 변경, 필요한 정보 변경

레코드 집합 추가

azureadmininc.org

이름

helloworld

✓

.azureadmininc.org

유형

A

▼

별칭 레코드 집합 ⓘ

☐ 예 ☒ 아니요

TTL *

1

TTL 단위

시간

▼

IP 주소

0.0.0.0

...

프라이빗 DNS 영역에 대한 계획

사용자 지정 도메인 이름 사용

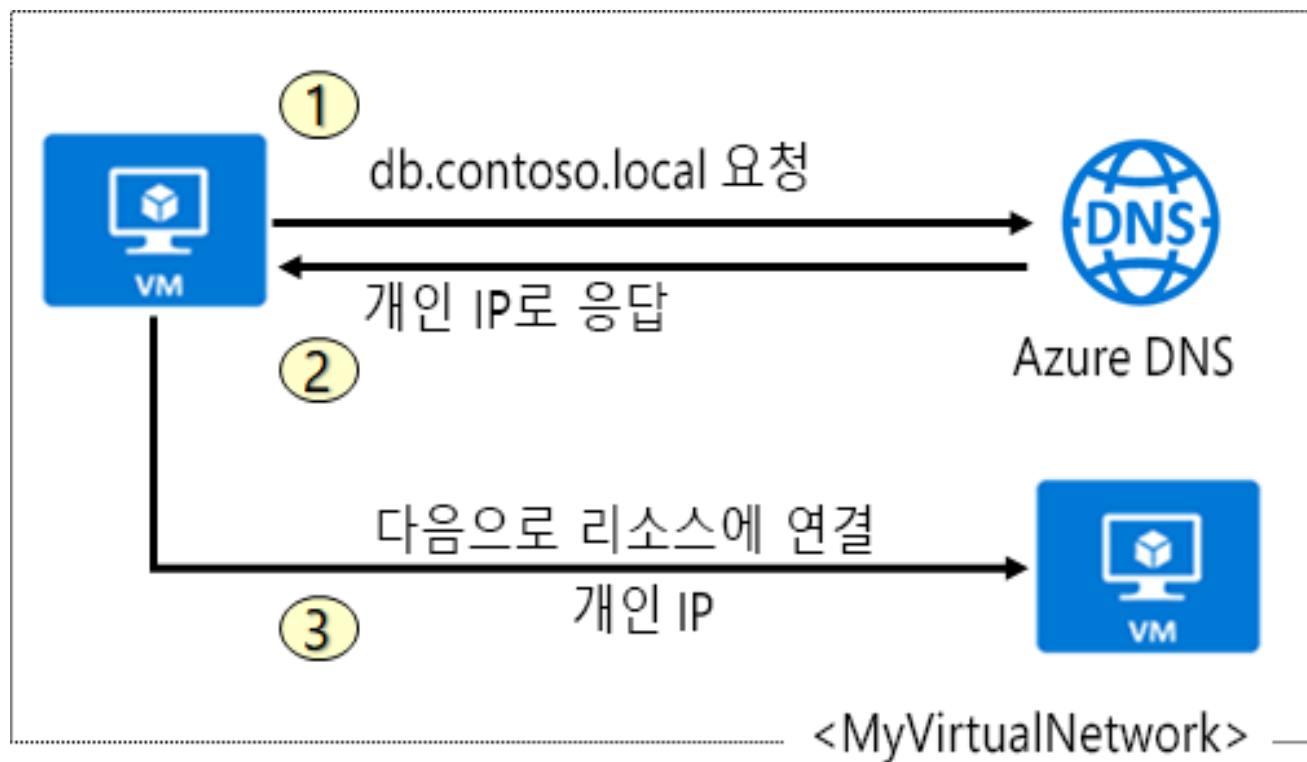
VNet 내 및 VNet 간 VM에 대한 이름 확인 제공.

호스트 이름 레코드 자동 관리

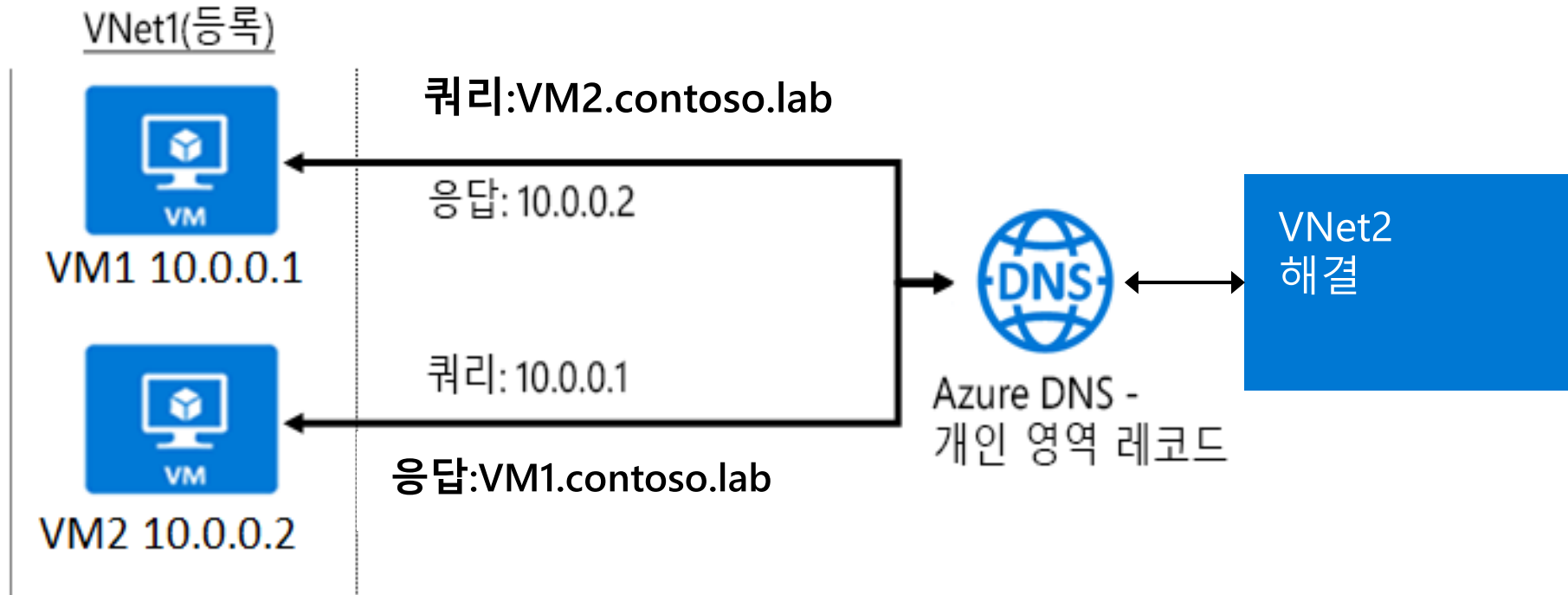
사용자 지정 DNS 솔루션이 필요하지 않습니다.

모든 공통 DNS 레코드 유형을 사용합니다.

모든 Azure 지역에서 사용할 수 있습니다.



프라이빗 영역 시나리오 확인

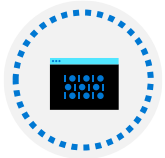


VNet1의 DNS 확인은 프라이빗으로서 인터넷에서 액세스할 수 없습니다.

가상 네트워크 전반에 걸쳐 DNS 쿼리가 확인됩니다.

역방향 DNS 쿼리는 동일한 가상 네트워크로 범위가 조정됩니다.

데모 - DNS



DNS 영역 만들기



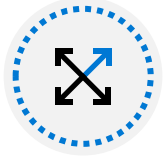
DNS 레코드 집합 추가



PowerShell을 사용하여 DNS 정보 보기



이름 서버 보기



해결 테스트



DNS 메트릭 살펴보기

요약 및 리소스 - Azure DNS 구성

지식 점검



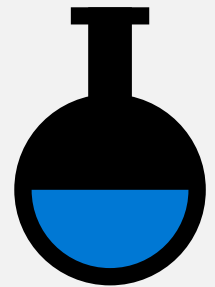
Microsoft Learn 모듈(docs.microsoft.com/ko-kr/Learn)

[Azure DNS에서 도메인 호스트\(샌드박스\)](#)

[Windows Server IaaS VM용 DNS 구현](#)

샌드박스는 실습 연습을 나타냅니다.

랩 04 - 가상 네트워크 구현



랩 04 - 가상 네트워킹 구현

랩 시나리오

Azure에 가상 네트워크를 만들어 Azure 가상 머신 몇 대를 호스트하려 합니다. 이들은 가상 네트워크의 다른 서브넷에 배포할 것입니다. 또한 프라이빗 및 공용 IP 주소가 시간이 흘러도 변경되지 않도록 하려고 합니다. Contoso 보안 요구 사항을 준수하려면 인터넷에서 액세스할 수 있는 Azure 가상 머신의 공용 엔드포인트를 보호해야 합니다. 마지막으로 가상 네트워크와 인터넷 모두에서 Azure 가상 머신에 대한 DNS 이름 확인을 구현해야 합니다.

목표

작업 1:

가상 네트워크
만들기 및 구성

작업 2

가상 네트워크에
가상 머신 배포

작업 3:

Azure VM의 개인
및 공용 IP 주소 구성

작업 4:

네트워크 보안
그룹 구성

작업 5:

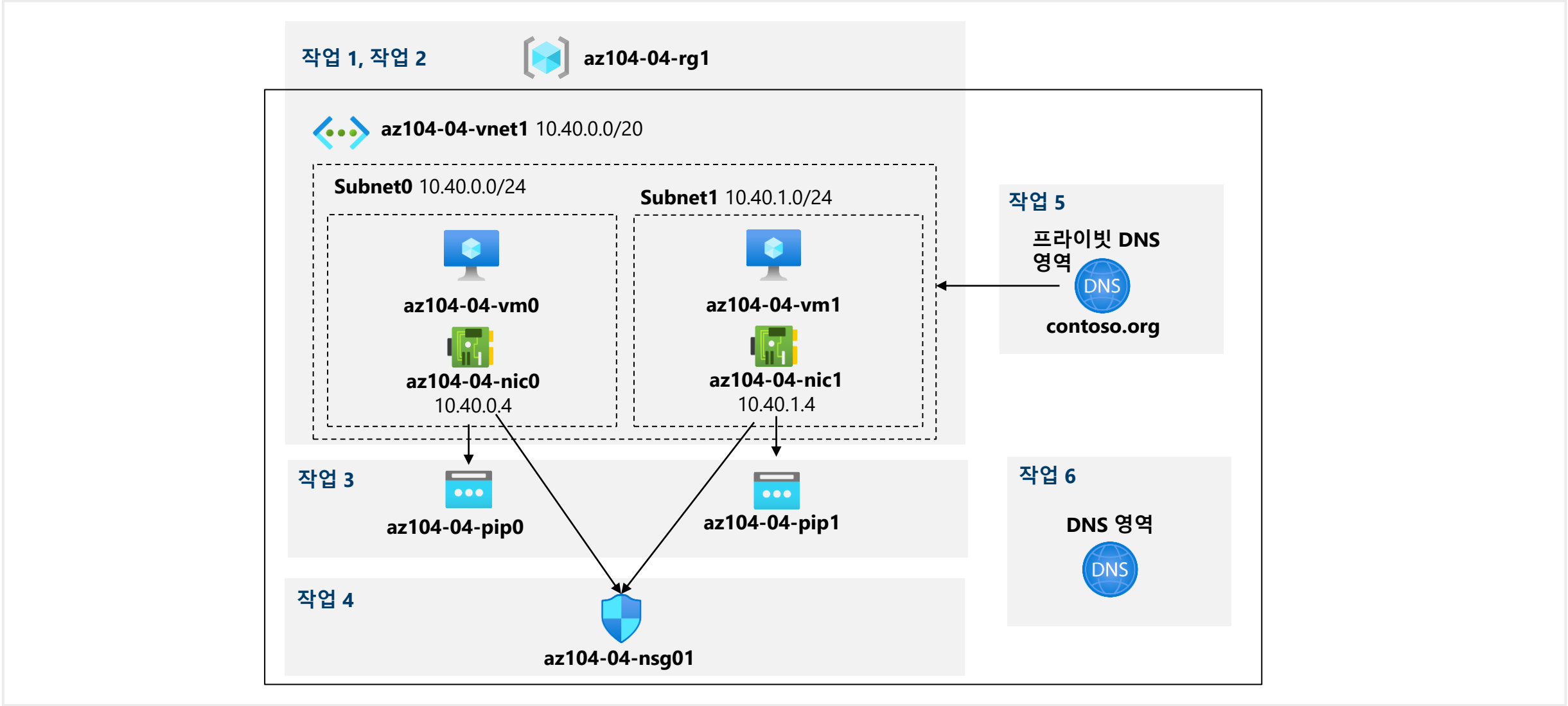
내부 이름 확인용
Azure DNS 구성

작업 6:

외부 이름 확인용
Azure DNS 구성

다음 슬라이드에서 아키텍처 다이어그램을 확인할 수 있습니다. ➔

랩 04 - 아키텍처 다이어그램



프레젠테이션 종료

