한국 마이크로소프트

Microsoft Technical Trainer

Enterprise Skills Initiative

AZ-104. Challenge Lab 04

LAB 04. 보안 Azure 가상 머신 네트워크 구현

Microsoft

이 문서는 Microsoft Technical Trainer팀에서 ESI 교육 참석자분들에게 제공해 드리는 문서입니다.

요약

이 내용들은 표시된 날짜에 Microsoft에서 검토된 내용을 바탕으로 하고 있습니다. 따라서, 표기된 날짜 이후에 시장의 요구사항에 따라 달라질 수 있습니다. 이 문서는 고객에 대한 표기된 날짜 이후에 변화가 없다는 것을 보증하지 않습니다.

이 문서는 정보 제공을 목적으로 하며 어떠한 보증을 하지는 않습니다.

문서 작성 연혁

날짜	버전	작성자	변경 내용
2023.08.27	1.0.0	우진환	LAB 04 내용 작성

목차

도전 과제

이 실습에서는 Azure 가상 머신을 위한 보안 네트워크를 만듭니다.

- 새 애플리케이션 보안 그룹을 사용하여 대상을 백 엔드 서브넷으로만 필터링하도록 기존 인바운드 보안 규칙을 재구성한 다음 방화벽과 라우팅 테이블을 생성합니다.
- 애플리케이션 규칙을 사용하여 방화벽을 구성한 다음 DNS 쿼리를 허용하는 네트워크 규칙을 추가합니다.
- Network Watcher를 지원하도록 Azure를 구성합니다.

STEP 01. 애플리케이션 보안 그룹 구성

1. "app-backend-asg" 이름의 애플리케이션 보안 그룹을 만듭니다.
2. VM1, VM2 가상 머신이 실행 중인지 확인합니다.
3. "app-backend-asg" 애플리케이션 보안 그룹을 VM2에 연결합니다.
4. "app-vnet-nsg" 네트워크 보안 그룹의 "AllowSsh" 인바운드 보안 규칙에서 대상 주소를 "app-backend-asg" 애플리케이션 보안 그룹으로 업데이트합니다.

STEP 02. 방화벽 및 경로 테이블 만들기

1. "app-vnet" 가상 네트워크에 10.1.63.0/24 주소 범위를 가지는 AzureFirewallSubnet 이름의 서브넷을 만듭니다.
2. 다음 속성을 사용하여 Azure Firewall을 만듭니다.

속성	값
리소스 그룹	RG1
이름	app-vnet-firewall
방화벽 SKU	표준
방화벽 관리	방화벽 규칙(클래식)을 사용하여 이 방화벽 관리
가상 네트워크 선택	기존 항목 사용
가상 네트워크	app-vnet (RG1)
공용 IP 주소	"새로 추가"를 선택한 후 fwpip33435474 이름 사용

3. Azure Firewall의 프라이빗 IP 주소와 퍼블릭 IP 주소를 확인합니다.
4. "app-vnet-firewall-rt" 이름의 경로 테이블을 만듭니다.
5. "app-vnet-firewall-rt" 경로 테이블에 다음 속성을 사용하여 새 경로를 만듭니다.

속성	값
경로 이름	to-firewall
대상 유형	IP 주소
대상 IP 주소/CIDR 범위	0.0.0.0/0
다음 홉 형식	가상 어플라이언스
다음 홉 주소	Azure Firewall 의 프라이빗 IP

6. "app-vnet-firewall-rt" 경로 테이블을 app-vnet의 frontend와 backend 서브넷에 연결합니다.

STEP 03. 방화벽 구성

1. Azure Firewall에서 다음 속성을 사용하여 애플리케이션 규칙 집합을 만듭니다.

속성	값
이름	app-vnet-fw-arc-web
우선 순위	200
대상 FQDN 이름	AllowAzurePipelines
소스	10.1.0.0/23
프로토콜:포트	https
대상 FQDN	dev.azure.com, azure.microsoft.com

2. Azure Firewall에 다음 속성을 사용하여 네트워크 규칙 집합을 만듭니다.

속성	값
이름	app-vnet-fw-nrc-dns
우선 순위	200
IP 주소 이름	AllowDns
프로토콜	UDP
소스	10.1.0.0/23
대상 주소	1.1.1.1, 1.0.0.1
대상 포트	53

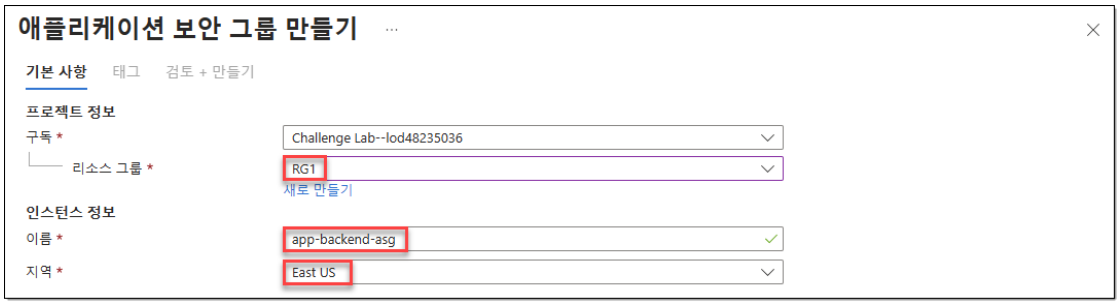
STEP 04. Network Watcher 지원을 위해 Azure 구성

1. "networkwatchersa<xxxxxxxx>" 이름의 스토리지 계정을 (US) Central US 지역에 만듭니다.
2. 자신의 구독에 Microsoft.Insights 리소스 공급자를 등록합니다.
3. 자신의 구독에 Microsoft.OperationalInsights 리소스 공급자를 등록합니다.
4. Central US 지역에 Network Watcher를 활성화합니다.

TASK 01. 애플리케이션 보안 그룹 구성

1. Azure 포털의 검색창에서 "애플리케이션 보안 그룹"을 검색한 후 클릭합니다. [애플리케이션 보안 그룹] 블레이드에서 [만들기]를 클릭합니다.

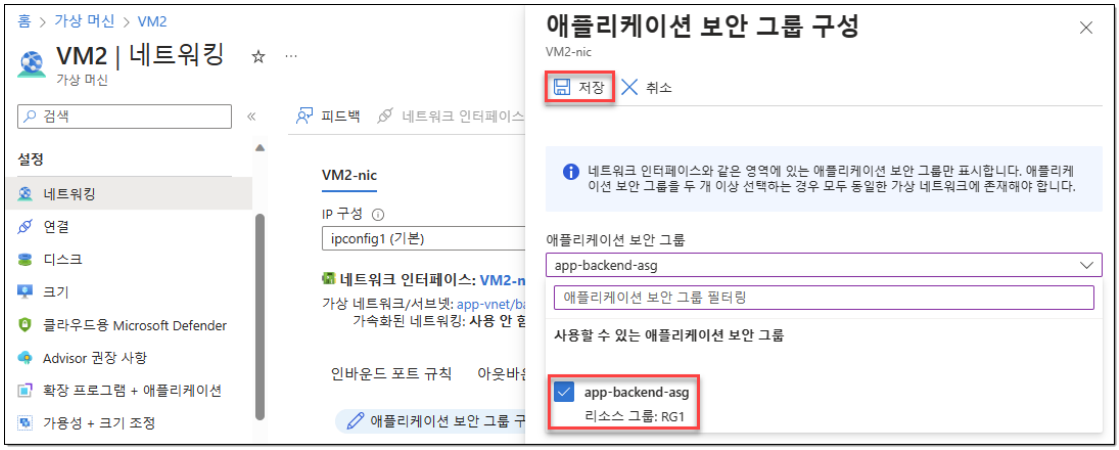
2. [애플리케이션 보안 그룹 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: RG1
   - [인스턴스 정보 - 이름]: app-backend-asg
   - [인스턴스 정보 - 지역]: East US



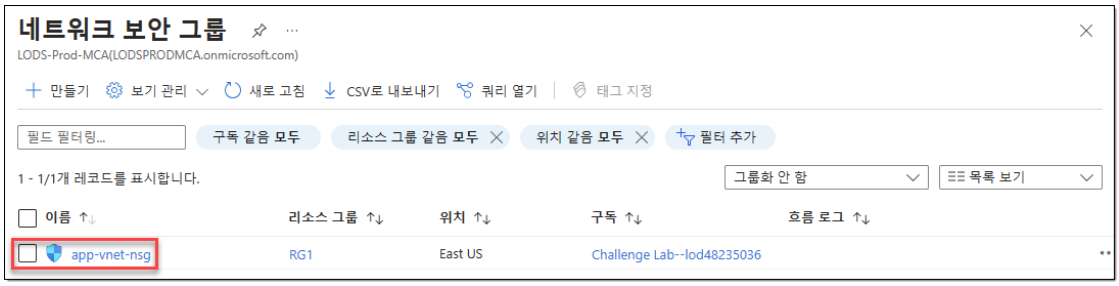
3. Azure 포털의 검색창에서 "가상 머신"을 검색한 후 클릭합니다. [가상 머신] 블레이드에서 VM1, VM2 가상 머신이 모두 "실행 중" 상태인지 확인합니다. VM2 가상 머신을 클릭합니다.

4. [VM2 가상 머신] 블레이드의 [설정 - 네트워킹]으로 이동한 후 [애플리케이션 보안 그룹] 탭을 클릭합니다. [애플리케이션 보안 그룹 구성]을 클릭합니다.

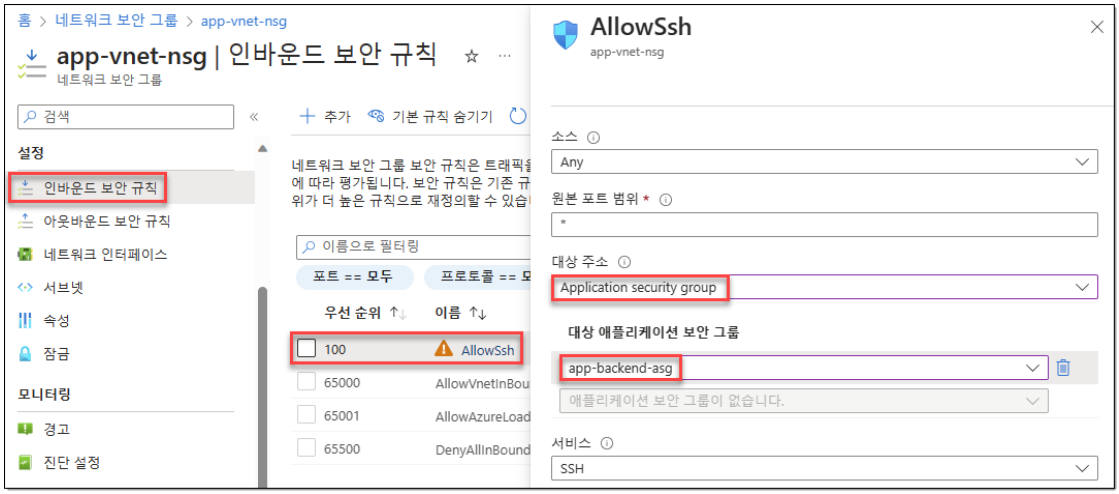
5. [애플리케이션 보안 그룹 구성] 창에서 "app-backend-asg" 애플리케이션 보안 그룹을 선택한 후 [저장]을 클릭합니다.



6. Azure 포털의 검색창에서 "네트워크 보안 그룹"을 검색한 후 클릭합니다. [네트워크 보안 그룹] 블레이드에서 app-vnet-nsg 네트워크 보안 그룹을 클릭합니다.

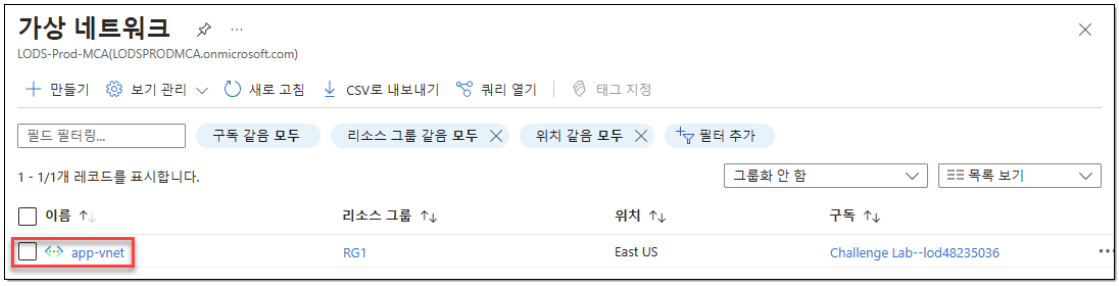


7. [app-vnet-nsg 네트워크 보안 그룹] 블레이드의 [설정 - 인바운드 보안 규칙]으로 이동한 후 "AllowSsh" 보안 규칙을 클릭합니다. [AllowSsh] 창에서 다음 두 설정을 변경한 후 [저장]을 클릭합니다.
   - 대상 주소: Application security group
   - 대상 애플리케이션 보안 그룹: app-backend-asg



TASK 02. 방화벽 및 경로 테이블 만들기

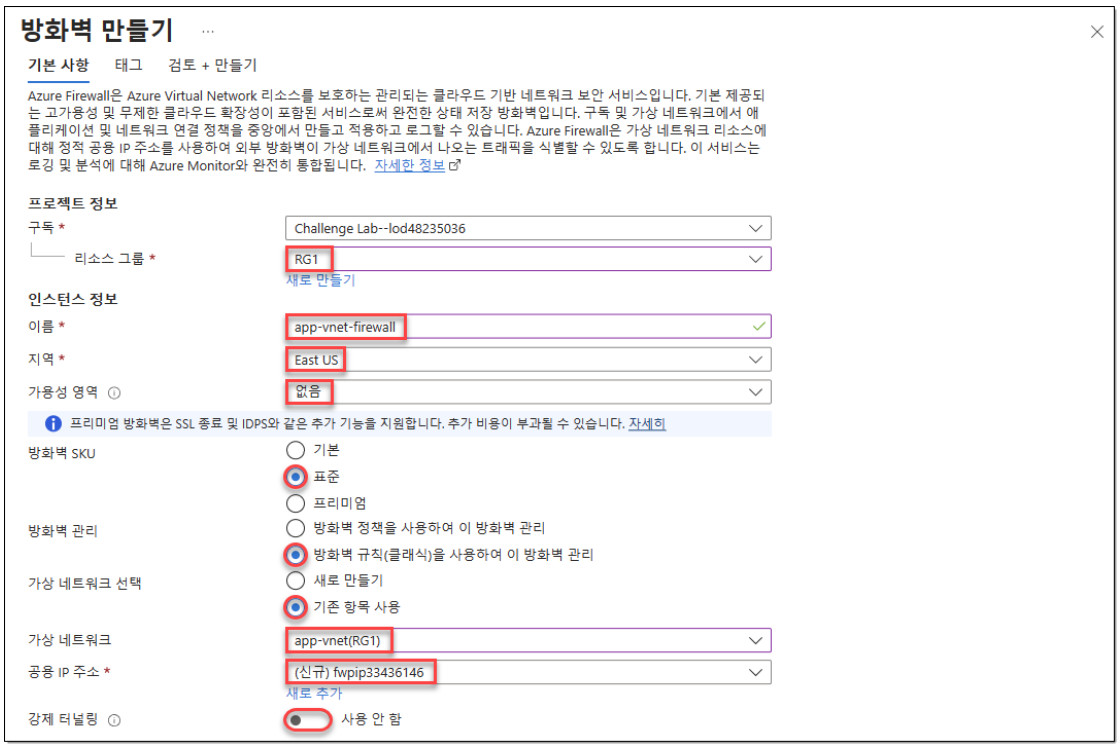
1. Azure 포털에서 "가상 네트워크"를 검색한 후 클릭합니다. [가상 네트워크] 블레이드에서 app-vnet 가상 네트워크를 클릭합니다.



2. [app-vnet 가상 네트워크] 블레이드의 [설정 - 서브넷]으로 이동한 후 메뉴에서 [서브넷]을 클릭합니다. [서브넷 추가] 창에서 아래와 같이 구성한 후 [저장]을 클릭합니다.
   - 이름: AzureFirewallSubnet
   - 서브넷 주소 범위: 10.1.63.0/24

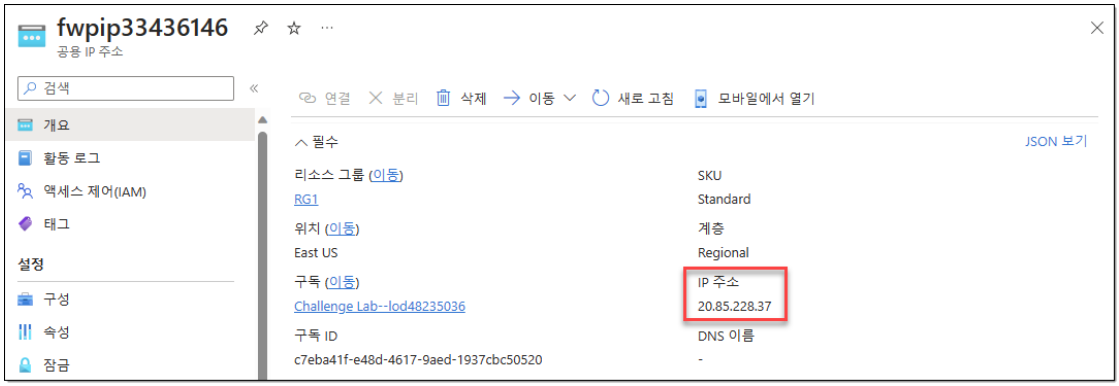
3. Azure 포털의 검색창에서 "방화벽"을 검색한 후 클릭합니다. [방화벽] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

4. [방화벽 만들기] 블레이드의 [기본 사항] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: RG1
   - [인스턴스 정보 - 이름]: app-vnet-firewall
   - [인스턴스 정보 - 지역]: East US
   - [인스턴스 정보 - 가용성 영역]: 없음
   - [인스턴스 정보 - 방화벽 SKU]: 표준
   - [인스턴스 정보 - 방화벽 관리]: 방화벽 규칙(클래식)을 사용하여 이 방화벽 관리
   - [인스턴스 정보 - 가상 네트워크 선택]: 기존 항목 사용
   - [인스턴스 정보 - 가상 네트워크]: app-vnet(RG1)
   - [인스턴스 정보 - 공용 IP 주소]: "새로 추가" 링크를 클릭한 후 "fwpip<xxxxxxxx>" 이름을 입력합니다.
   - [인스턴스 정보 - 강제 터널링]: 사용 안 함

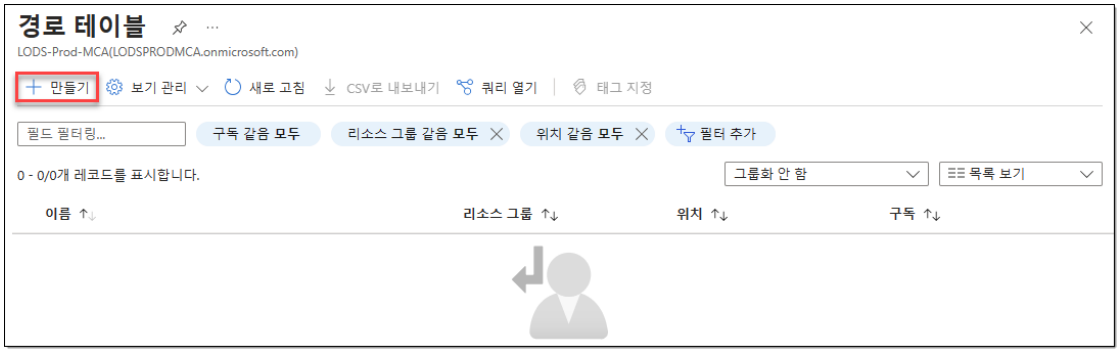


5. 배포한 [app-vnet-firewall 방화벽] 블레이드의 [개요]로 이동합니다. 표시되는 방화벽 프라이빗 IP를 메모장에 기록합니다. 방화벽 퍼블릭 IP의 이름 링크를 클릭합니다.

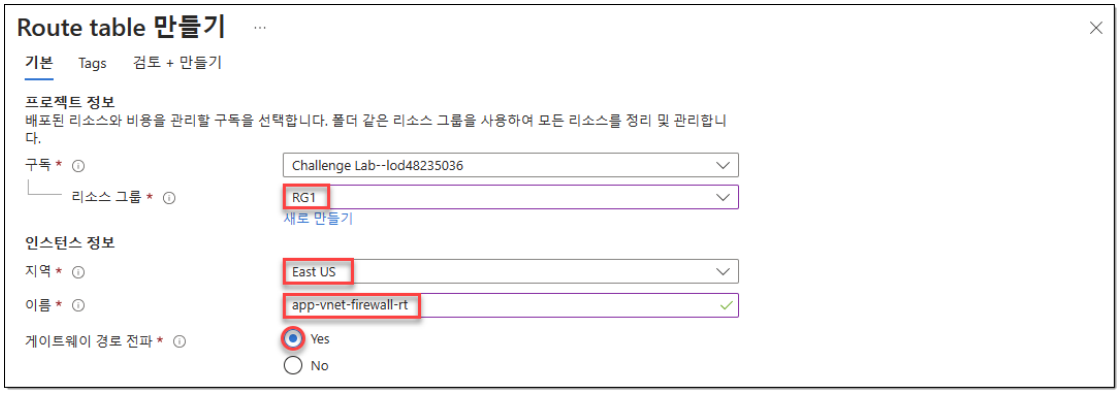
6. [fwpip<xxxxxxxx> 공용 IP 주소] 블레이드의 [개요]에서 표시되는 IP 주소를 메모장에 기록합니다.



7. Azure 포털의 검색창에서 "경로 테이블"을 검색한 후 클릭합니다. [경로 테이블] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

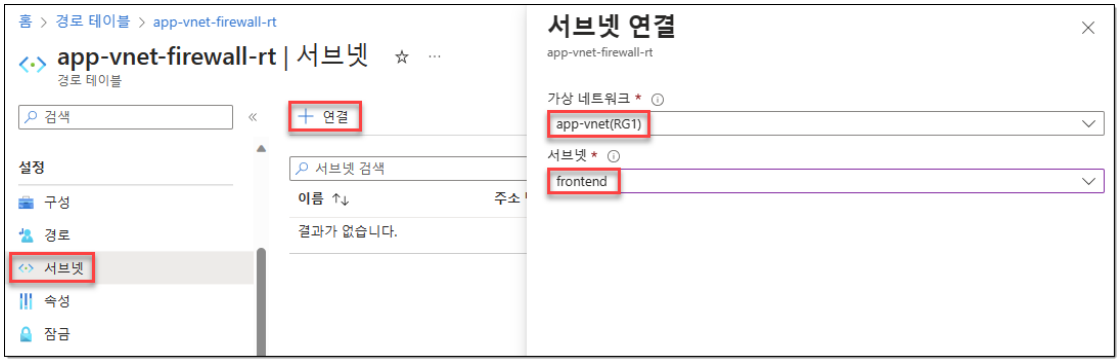


8. [Route table 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토 + 만들기]를 클릭합니다. [검토 + 만들기] 탭에서 [만들기]를 클릭합니다.
   - [프로젝트 정보 - 리소스 그룹]: RG1
   - [인스턴스 정보 - 지역]: East US
   - [인스턴스 정보 - 이름]: app-vnet-firewall-rt
   - [인스턴스 정보 - 게이트웨이 경로 전파]: Yes

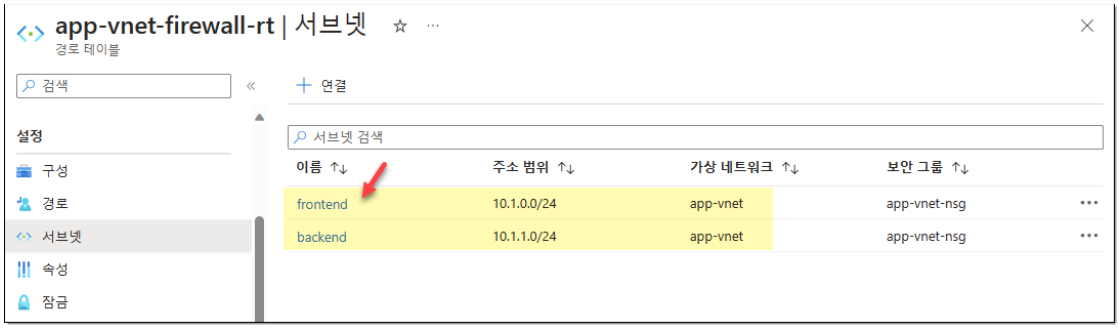


9. 새로 만든 [`app-vnet-firewall-rt` 경로 테이블] 블레이드의 [설정 - 경로]로 이동한 후 메뉴에서 [추가]를 클릭합니다. [경로 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.
   - 경로 이름: to-firewall
   - 대상 유형: IP 주소
   - 대상 IP 주소/CIDR 범위: 0.0.0.0/0
   - 다음 홉 형식: 가상 어플라이언스
   - 다음 홉 주소: 메모장에 복사했던 방화벽의 프라이빗 IP 주소를 입력합니다.

10. [`app-vnet-firewall-rt` 경로 테이블] 블레이드의 [설정 - 서브넷]으로 이동한 후 메뉴에서 [연결]을 클릭합니다. [서브넷 연결] 창에서 다음과 같이 구성한 후 [확인]을 클릭합니다.
    - 가상 네트워크: app-vnet(RG1)
    - 서브넷: frontend



11. 동일한 방법으로 `app-vnet` 가상 네트워크의 `backend` 서브넷도 연결합니다.



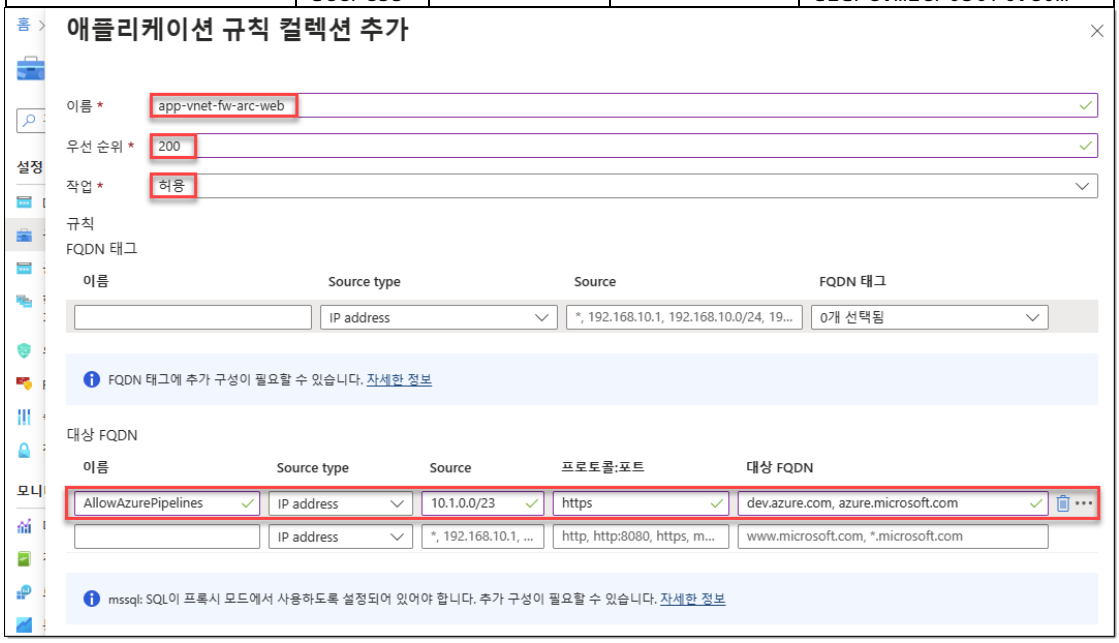
TASK 03. 방화벽 구성

1. Azure 포털의 검색창에서 "`방화벽`"을 검색한 후 클릭합니다. [방화벽] 블레이드에서 `app-vnet-firewall` 방화벽 리소스를 클릭합니다.

2. [`app-vnet-firewall` 방화벽] 블레이드의 [설정 - 규칙(클래식)]으로 이동합니다. [애플리케이션 규칙 컬렉션] 탭에서 [애플리케이션 규칙 컬렉션 추가]를 클릭합니다.

3. [애플리케이션 규칙 컬렉션 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.
   - 이름: app-vnet-fw-arc-web
   - 우선 순위: 200
   - 작업: 허용
   - 대상 FQDN 영역에 다음과 같은 구성을 설정합니다.

이름	Source type	Source	프로토콜:포트	대상 FQDN
AllowAzurePipelines	IP address	10.1.0.0/23	https	dev.azure.com, azure.microsoft.com

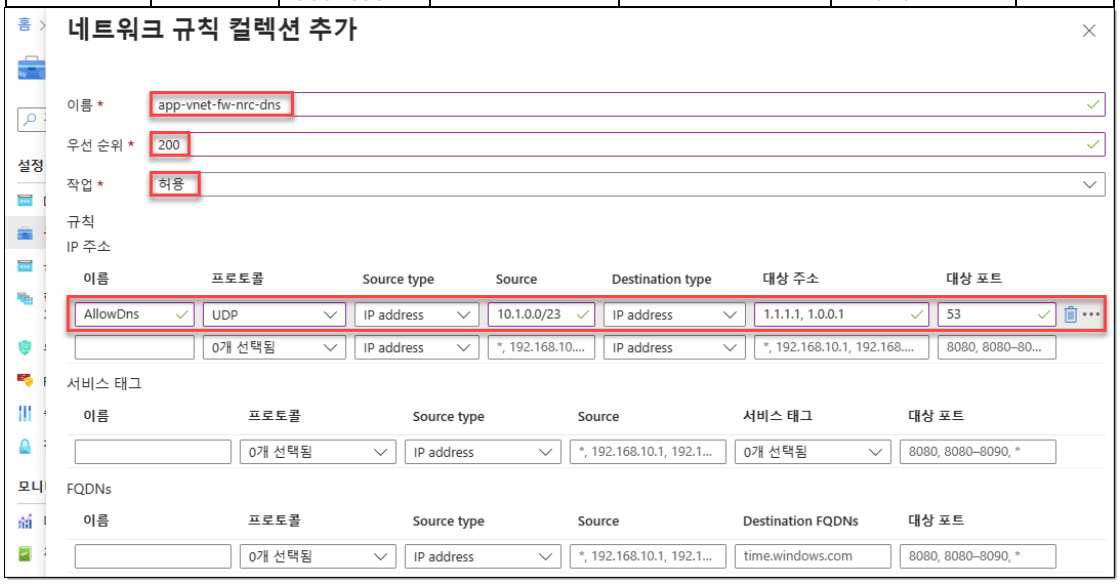


4. [app-vnet-firewall 방화벽 | 규칙(컬렉션)] 블레이드의 [네트워크 규칙 컬렉션] 탭으로 이동한 후 [네트워크 규칙 컬렉션 추가]를 클릭합니다.

5. [네트워크 규칙 컬렉션 추가] 창에서 아래와 같이 구성한 후 [추가]를 클릭합니다.
   - 이름: app-vnet-fw-nrc-dns
   - 우선 순위: 200
   - 작업: 허용
   - IP 주소에서 다음과 같이 구성합니다.

이름	프로토콜	Source type	Source	Destination type	대상 주소	대상 포트

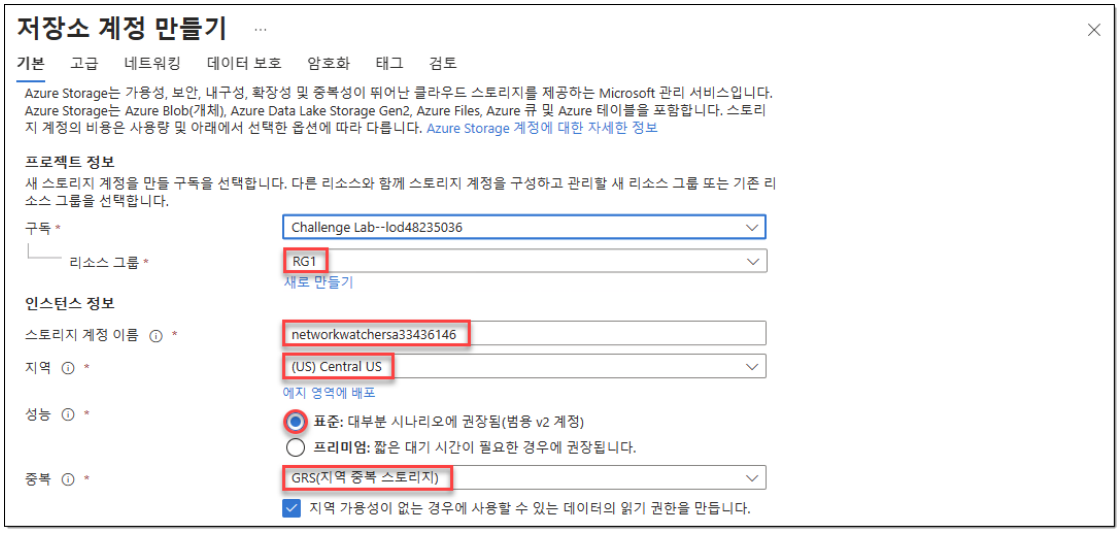
AllowDns	UDP	IP address	10.1.0.0/23	IP address	1.1.1.1, 1.0.0.1	53



TASK 04. Network Watcher 지원을 위해 Azure 구성

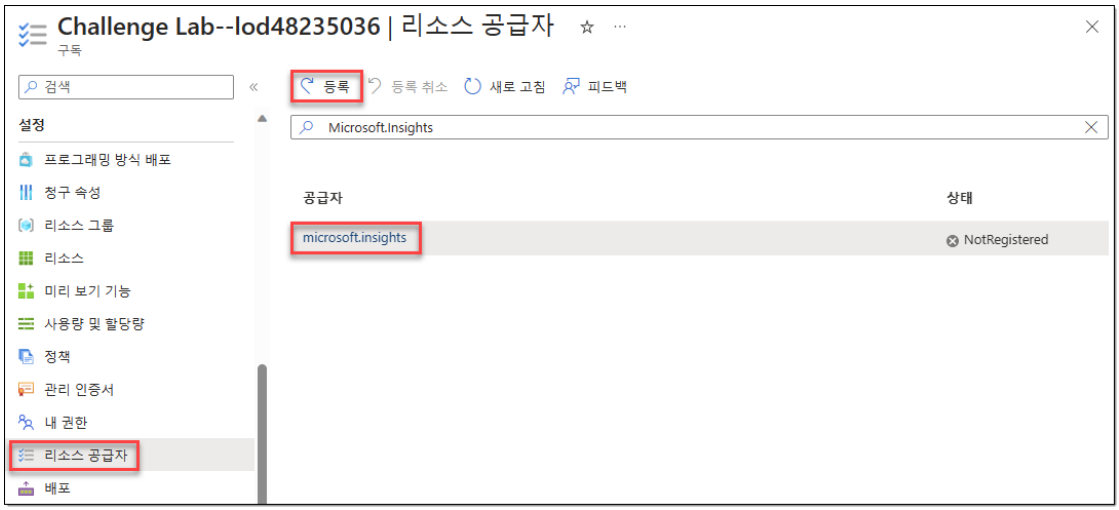
1. Azure 포털의 검색창에서 "스토리지 계정"을 검색한 후 클릭합니다. [스토리지 계정] 블레이드의 메뉴에서 [만들기]를 클릭합니다.

2. [저장소 계정 만들기] 블레이드의 [기본] 탭에서 아래와 같이 구성한 후 [검토]를 클릭합니다. [검토] 탭에서 [만들기]를 클릭합니다. Network Watcher에서 네트워크 보안 그룹의 흐름 로그를 구현하기 위해서는 로그가 저장될 스토리지 계정을 만들어야 합니다.
   - [프로젝트 정보 - 리소스 그룹]: RG1
   - [인스턴스 정보 - 스토리지 계정 이름]: `networkwatchersa<xxxxxxxx>`
   - [인스턴스 정보 - 지역]: (US) Central US
   - [인스턴스 정보 - 성능]: 표준
   - [인스턴스 정보 - 중복]: GRS(지역 중복 스토리지)

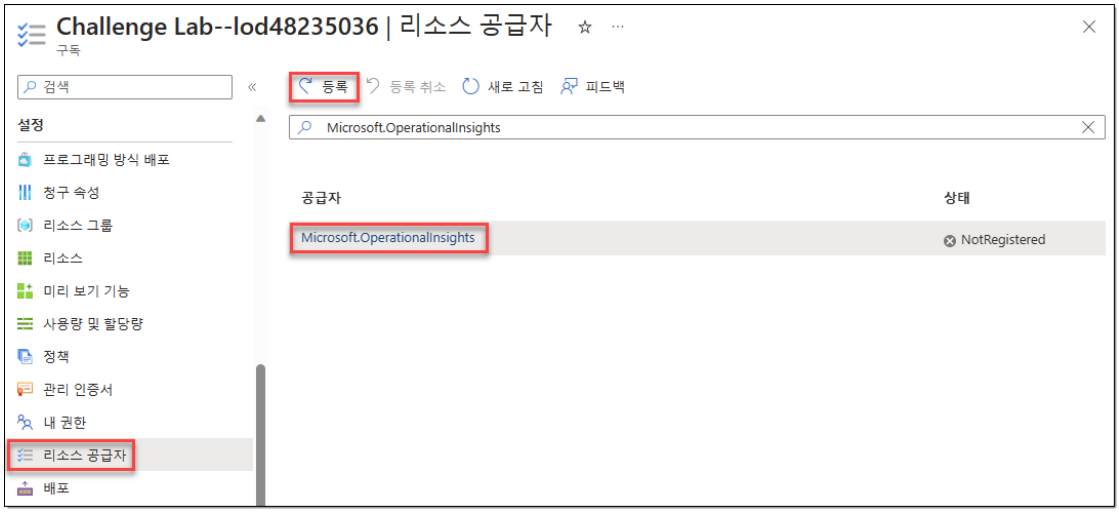


3. Azure 포털의 검색창에서 "구독"을 검색한 후 클릭합니다. [구독] 블레이드에서 자신의 구독을 클릭합니다.

4. [구독] 블레이드의 [설정 - 리소스 공급자]로 이동합니다. 검색창에서 "`Microsoft.Insights`"를 검색한 후 선택하고 메뉴에서 [등록]을 클릭합니다.



5. 동일한 방법으로 "`Microsoft.OperationalInsights`" 리소스 공급자도 검색한 후 [등록]을 클릭합니다.



6. Azure 포털의 검색창에서 "`Network Watcher`"를 검색한 후 클릭합니다. [Network Watcher] 블레이드의 [개요]에서 [추가]를 클릭합니다. [Network Watcher 추가] 창에서 "`(US) Central US`"를 선택한 후 [추가]를 클릭합니다.