네트워크 보안 그룹(NSG)을 통해 네트워크 트래픽 필터링(Subnet에 연결)

주신영 bit1010@live.com

이번 실습은 MS의 실습 자료를 참고하였습니다.

자습서: Azure Portal을 사용하여 네트워크 보안 그룹을 통해 네트워크 트래픽 필터링

지역은 계정에 제한이 없다면 Korea Central을 선택합니다.

네트워크 보안 그룹은 가상머신의 네트워크 인터페이스 카드(NIC)에 직접 연결하거나 서브넷에 연결해서 사용할 수 있습니다.

이번 실습에서는 네트워크 보안 그룹을 가상 네트워크의 서브넷과 연결해서 사용해보겠습니다.

네트워크 보안 그룹(NSG)을 통해 네트워크 트래픽 필터링(NIC에 연결)을 먼저 진행합니다.

가상 네트워크 만들기

1. Azure Portal 메뉴에서 **+ 리소스 만들기**>**네트워킹**>**Virtual Network**를 선택하거나 포털 검색 상자에서 *Virtual Network*를 검색합니다.
2. **만들기**를 선택합니다.
3. **가상 네트워크 만들기**의 **기본** 탭에서 다음 정보를 입력하거나 선택합니다.

설정	값
프로젝트 세부 정보	

Resource group	**새로 만들기**를 선택합니다. *myNsgSubnetRG*을 입력합니다. **확인**을 선택합니다. * 리소스 그룹이 생성되어 있으면 선택합니다.
인스턴스 세부 정보	
이름	*myVNet*을 입력합니다.

4. **검토 + 만들기** 탭을 선택하거나 페이지 하단에 있는 파란색 **검토 + 만들기** 단추를 선택합니다.
5. **만들기**를 선택합니다.

네트워크 보안 그룹 만들기

NSG(네트워크 보안 그룹)는 가상 네트워크의 네트워크 트래픽을 보호합니다.

이전 실습에서는 가상머신 생성 시 공용 인바운드 포트를 사용하면 NSG가 각 1개씩 생성됐고 없음으로 하면 NSG없이 생성됐습니다. 이렇게 적용하면 NIC에 NSG가 연결됩니다.

서브넷에 연결하거나 인터넷으로 연결하는 포트가 필요없다면 NSG를 없음으로 설정하면 됩니다.

1. Azure Portal 메뉴에서 **+ 리소스 만들기**>**네트워킹**>**네트워크 보안 그룹**을 선택하거나 포털 검색 상자에서 *네트워크 보안 그룹*을 검색합니다.
2. **만들기**를 선택합니다.
3. **네트워크 보안 그룹 만들기**의 **기본** 탭에서 다음 정보를 입력하거나 선택합니다.

설정	값
프로젝트 세부 정보	
Resource group	***myNsgSubnetRG***을 선택합니다.
인스턴스 세부 정보	
속성	*myNSG*를 입력합니다.

4. **검토 + 만들기** 탭을 선택하거나, 페이지 아래쪽에서 파란색 **검토 + 만들기** 단추를 선택합니다.
5. **만들기**를 선택합니다.

서브넷에 네트워크 보안 그룹 연결

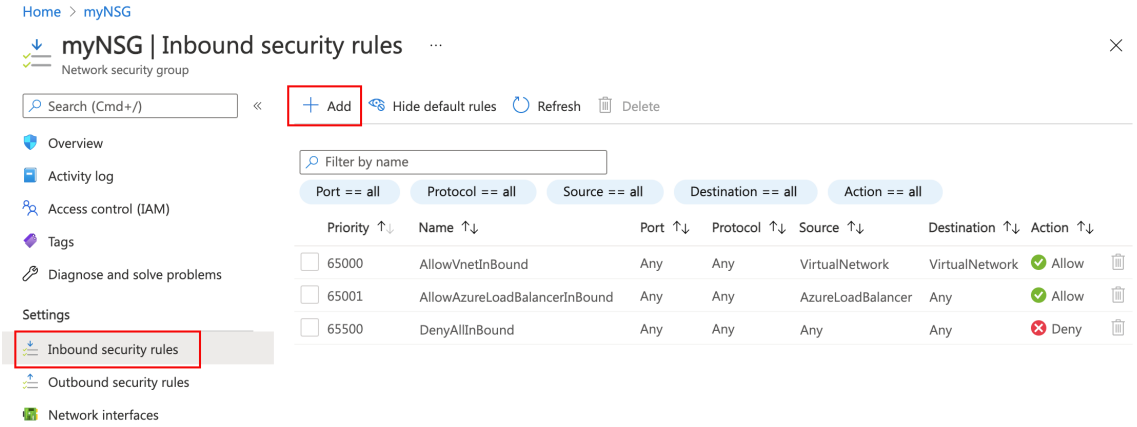
네트워크 보안 그룹(NSG)을 이전에 만든 가상 네트워크의 서브넷과 연결합니다. 서브넷과 연결하게 되면 해당 서브넷에 연결되는 가상머신은 네트워크 보안그룹의 설정이 자동으로 적용됩니다.

1. 포털 검색 상자에서 *myNsg*를 검색합니다.
2. **myNSG**의 **설정** 섹션에서 **서브넷**을 선택합니다.
3. **서브넷** 페이지에서 **+ 연결**을 선택합니다.

4. **서브넷 연결**에서 **가상 네트워크**에 대해 **myVNet**을 선택합니다.
5. **서브넷**에 대해 **default**를 선택한 다음 **확인**을 선택합니다.

보안 규칙 만들기

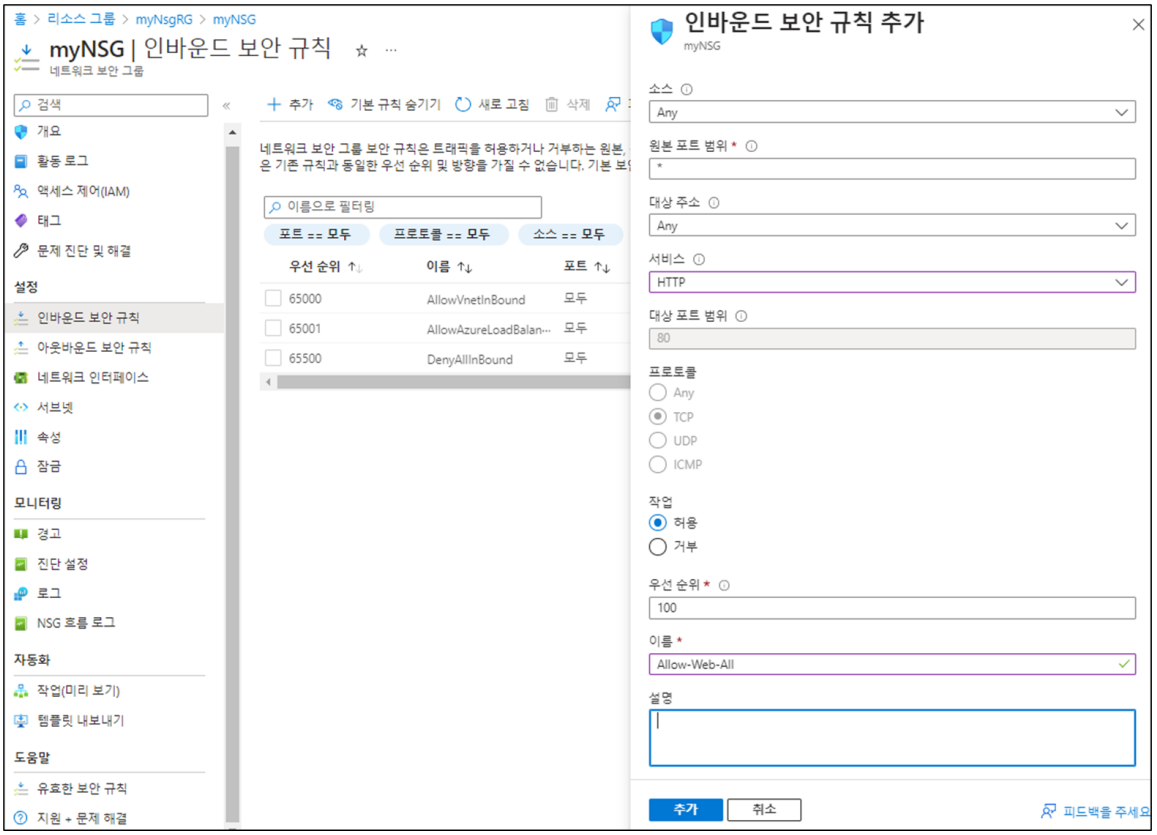
1. **myNSG**의 **설정** 섹션에서 **인바운드 보안 규칙**을 선택합니다.
2. **인바운드 보안 규칙** 페이지에서 **+ 추가**를 선택합니다.



3. **포트 80(HTTP)**를 허용하는 보안 규칙을 만듭니다.

   인바운드 보안 규칙 추가 페이지에서 다음 정보를 입력하거나 선택합니다.

설정	값
원본	**Any**(기본값)를 그대로 둡니다.
원본 포트 범위	**(*)**의 기본값을 그대로 둡니다.
대상	**Any**(기본값)를 그대로 둡니다.
서비스	**HTTP**을 선택합니다.
대상 포트 범위	*80*이 선택됩니다.
작업	**허용**(기본값)을 그대로 둡니다.
우선 순위	**100**(기본값)을 그대로 둡니다.
Name	*Allow-Web-All*을 입력합니다.



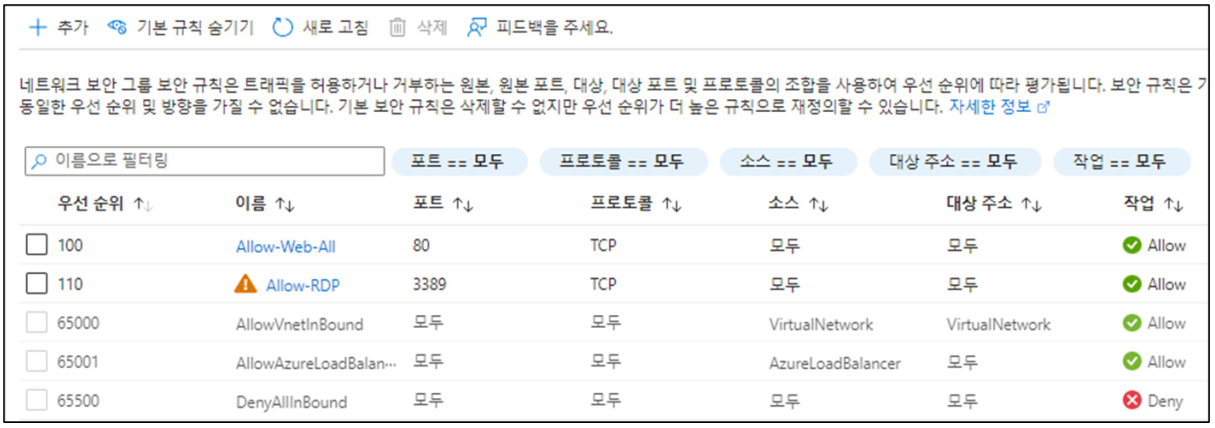
4. **추가**를 선택합니다.

5. **3389(RDP)**를 허용하는 보안 규칙을 만듭니다.
   다음 정보를 사용하여 3-4단계를 다시 완료합니다.

설정	값
원본	**모두**(기본값)를 그대로 둡니다.
원본 포트 범위	**(*)**의 기본값을 그대로 둡니다.
대상	**Any**(기본값)를 그대로 둡니다.
서비스	**RDP**을 선택합니다.
대상 포트 범위	*3389*이 선택됩니다.
작업	**허용**(기본값)을 그대로 둡니다.
우선 순위	**110**(기본값)을 그대로 둡니다.
Name	*Allow-RDP*을 입력합니다.

6. **추가**를 선택합니다.

1-3단계를 완료한 후 사용자가 만든 규칙을 검토합니다. 목록은 다음 예의 목록과 같습니다.



가상 머신 만들기

가상 네트워크에 두 개의 VM(가상 머신)을 만듭니다.

첫 번째 가상 머신 만들기

웹서버로 사용 할 가상 머신을 추가합니다. 80포트를 사용해서 연결 할 예정입니다.

1. Azure Portal 메뉴에서 **+ 리소스 만들기>컴퓨팅>가상 머신**을 선택하거나 포털 검색 상자에서 *가상 머신*을 검색합니다.
2. **가상 머신 만들기**의 **기본** 탭에서 다음 정보를 입력하거나 선택합니다.

설정	값
프로젝트 세부 정보	
Resource group	***myNsgSubnetRG***을 선택합니다.
인스턴스 세부 정보	
가상 머신 이름	*myVMWeb*을 입력합니다.
가용성 옵션	기본값인 **인프라 중복 필요 없음**을 그대로 둡니다.
보안 유형	기본값인 **표준**을 그대로 둡니다.
이미지	**Windows Server 2022 Datacenter - Gen2**을 선택합니다.
관리자 계정	
사용자 이름	사용자 이름을 입력합니다.
암호	암호를 입력합니다.
암호 확인	암호를 다시 입력합니다.

3. **네트워킹** 탭을 선택합니다.
4. **네트워킹** 탭에서 다음 정보를 입력하거나 선택합니다.

설정	값
네트워크 인터페이스	
가상 네트워크	**myVNet**을 선택합니다.
서브넷	**default(10.0.0.0/24)** 을 선택합니다.
공용 IP	새 공용 IP(기본값)를 그대로 둡니다.
NIC 네트워크 보안 그룹 추가	**없음**을 선택합니다.

5. **검토 + 만들기** 탭을 선택하거나, 페이지 아래쪽에서 파란색 **검토 + 만들기** 단추를 선택합니다.
6. **만들기**를 선택합니다. VM을 배포하는 데 몇 분 정도 걸릴 수 있습니다.

> 💡 서브넷에 네트워크 보안 그룹(NSG)을 연결했으므로 **NIC 네트워크 보안 그룹**은 없음을 선택합니다.

두 번째 가상 머신 만들기

관리용 가상 머신을 추가합니다. 3389(RDP)를 사용해서 연결 할 예정입니다.

1~6단계를 다시 완료하되 2단계에서 가상 머신 이름에 *myVMMgmt*를 입력합니다.

다음 섹션으로 진행하기 전에 VM이 배포를 완료할 때까지 기다리세요.

가상 머신 보안 규칙 확인

1. 포털 검색 상자에서 *myVMWeb*를 검색합니다.
2. **myVMWeb**의 **설정** 섹션에서 **네트워크**를 선택합니다.
3. 인바운드 포트 규칙을 확인해보면 네트워크 보안 그룹에서 추가한 사항이 적용되어 있습니다.

4. *myVMMgmt*도 동일하게 적용되어 있음을 확인할 수 있습니다.

원격데스크탑(RDP) 연결 확인

1. 포털 검색 상자에서 *myVMMgmt*를 검색합니다.
2. **개요** 페이지에서 **연결** 단추를 선택한 다음 **RDP**를 선택합니다.
3. **RDP 파일 다운로드**를 선택합니다.
4. 다운로드한 rdp 파일을 열고 **연결**을 선택합니다. VM을 만들 때 지정한 사용자 이름과 암호를 입력합니다.
5. **확인**을 선택합니다.
6. 연결 프로세스 중에 인증서 경고를 받을 수 있습니다. 경고 메시지가 표시되면 **예** 또는 **계속**을 선택하여 연결을 계속합니다.
7. *myVMWeb*도 동일하게 연결합니다.

> 💡 현재 보안규칙은 *myVMWeb, myVMMgmt* 두개의 가상머신 모두 동일하게 적용되어 있으므로 *myVMWeb*도 동일하게 RDP로 접속 됩니다. 현 구성은 NSG가 서브넷에 연결되어 있고 동일한 NSG를 사용하므로 각각 다른 규칙을 사용하고 싶으면 ASG(애플리케이션 보안 그룹)를 각 가상머신에서 사용하도록 구성을 추가하면 됩니다.

현재 연결한 원격 데스크탑은 모두 종료하고 각 가상머신에서 다른 애플리케이션 포트 규칙을 사용하기 위한 설정을 추가하겠습니다.

애플리케이션 보안 그룹 만들기

ASG(애플리케이션 보안 그룹)를 사용하면 웹 서버와 같은 유사한 기능을 갖는 서버를 함께 그룹화할 수 있습니다.

1. Azure Portal 메뉴에서 **+ 리소스 만들기>네트워킹>애플리케이션 보안 그룹**을 선택하거나 포털 검색 상자에서 *애플리케이션 보안 그룹*을 검색합니다.
2. **만들기**를 선택합니다.

3. **애플리케이션 보안 그룹 만들기**의 **기본** 탭에서 다음 정보를 입력하거나 선택합니다.

설정	값
프로젝트 세부 정보	
Subscription	구독을 선택합니다.
Resource group	***myNsgSubnetRG***을 선택합니다.
인스턴스 세부 정보	
속성	*myAsgWebServers*를 입력합니다.

4. **검토 + 만들기** 탭을 선택하거나, 페이지 아래쪽에서 파란색 **검토 + 만들기** 단추를 선택합니다.
5. **만들기**를 선택합니다.
6. 다음 값을 지정하여 이전 단계를 반복합니다.

설정	값
프로젝트 세부 정보	
Resource group	***myNsgSubnetRG***을 선택합니다.
인스턴스 세부 정보	
속성	*myAsgMgmtServers*를 입력합니다.

7. **검토 + 만들기** 탭을 선택하거나, 페이지 아래쪽에서 파란색 **검토 + 만들기** 단추를 선택합니다.
8. **만들기**를 선택합니다.

보안 규칙 수정

1. myNSG **네트워크 보안 그룹**으로 이동하여 인바운드 보안 규칙에서 추가한 **Allow-Web-All**를 선택합니다. 대상 주소에서 *Application security group*를 선택합니다. *myAsgWebServers*를 선택하고 **저장**을 누릅니다.

   이렇게 적용하면 Allow-Web-All는 *myAsgWebServers* 애플리케이션 보안 그룹을 선택한 가상 머신만 HTTP 80포트를 허용합니다.

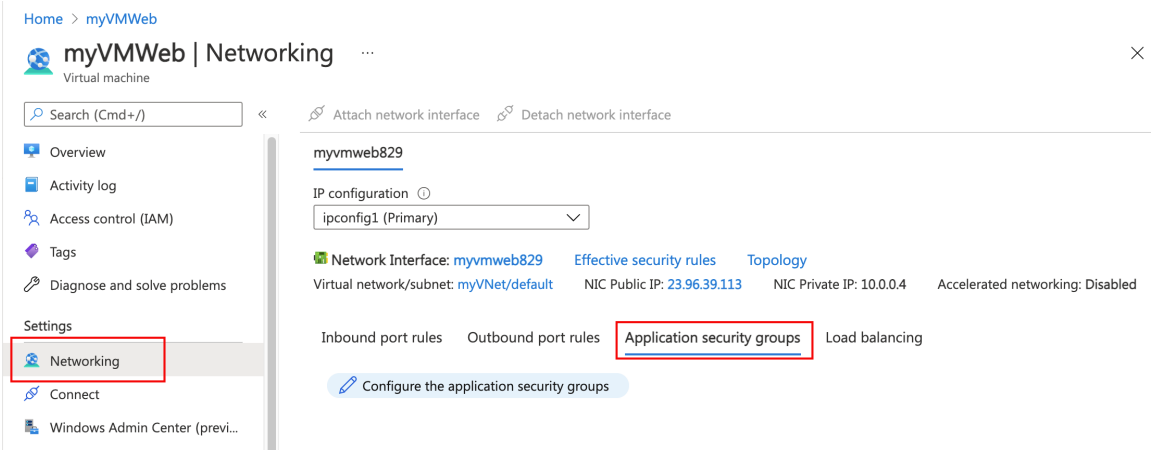
2. **Allow-RDP**도 *myAsgMgmtServers*를 동일하게 적용합니다.

***myVMWeb, myVMMgmt* 두개의 가상머신에 RDP로 접속해보면 연결이 되지 않는 걸 확인 할 수 있습니다.**

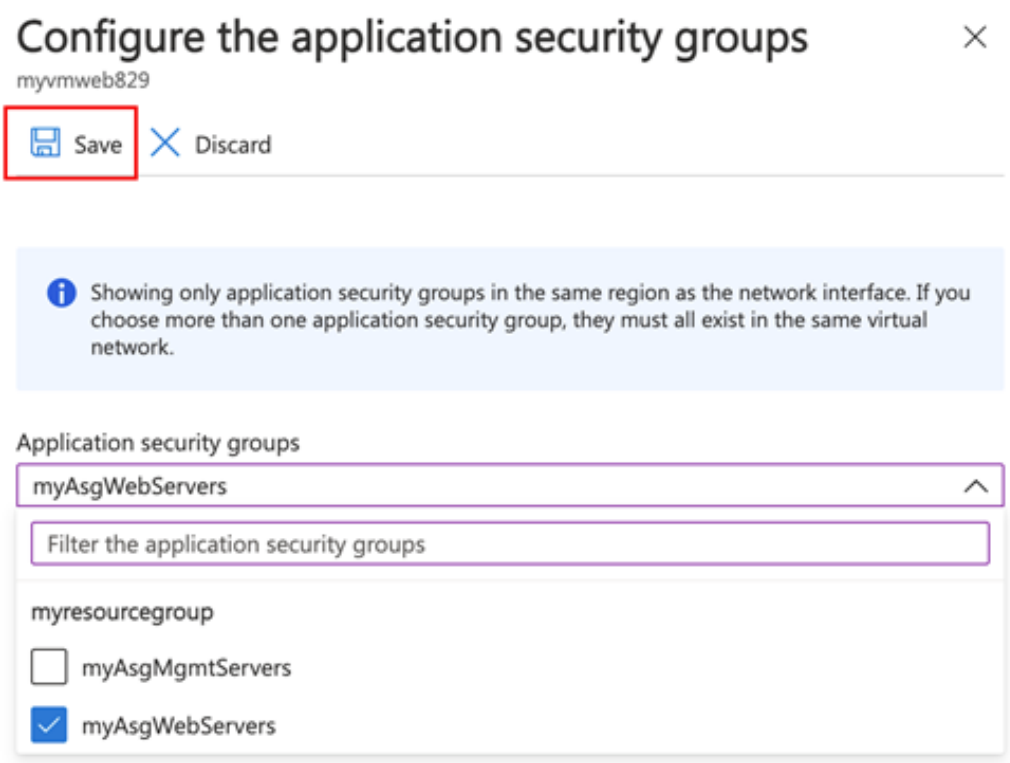
(대상이 변경됨)

네트워크 인터페이스를 ASG에 연결

1. 포털 검색 상자에서 *myVMWeb*을 검색합니다.
2. **myVMWeb** VM의 **설정** 섹션에서 **네트워킹**을 선택합니다.
3. **애플리케이션 보안 그룹** 탭을 선택한 다음, **애플리케이션 보안 그룹 구성**을 선택합니다.



4. **애플리케이션 보안 그룹 구성**에서 **myAsgWebServers**를 선택합니다. **저장**을 선택합니다.



5. *myVMMgmt* 가상 머신을 검색하고 **myAsgMgmtServers** ASG를 선택하여 3~4단계를 동일하게 적용합니다.

트래픽 필터 테스트

1. *myVMMgmt*로 원격 데스크탑(RDP)을 이용해서 접속합니다.
2. PowerShell 세션을 엽니다. 다음을 사용하여 **myVMWeb**에 연결합니다.

   ```
   mstsc /v:myVmWeb
   ```

   mstsc는 원격데스크탑의 실행파일 이름입니다.

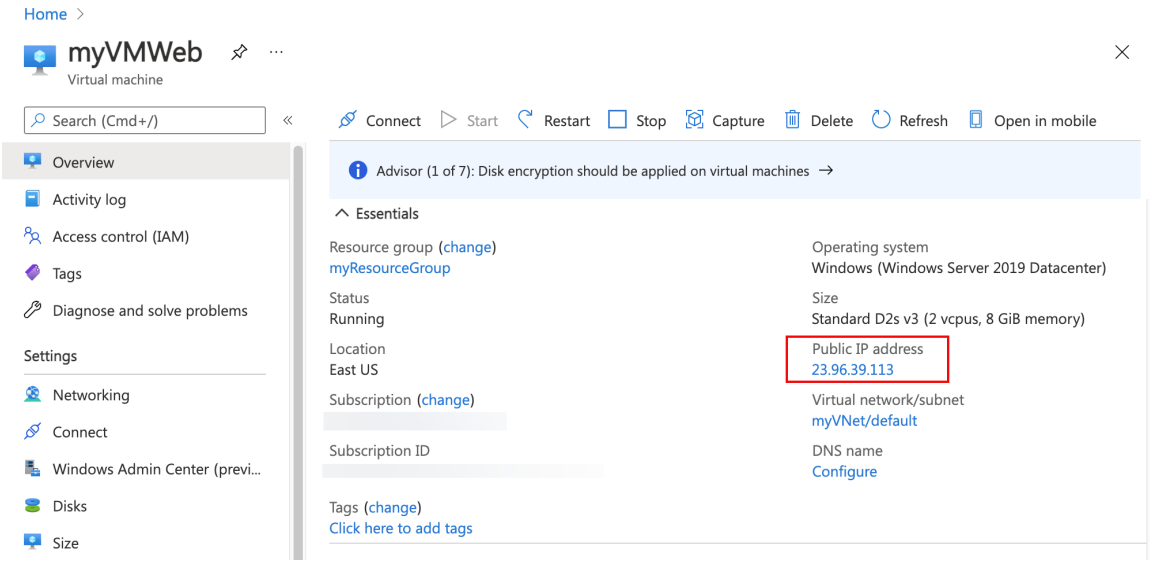
   로그인해서 접속합니다.

> 기본적으로 동일한 네트워크의 가상 머신에서 모든 포트를 통해 서로 통신할 수 있으므로 myVMMgmt에서 myVMWeb으로의 RDP 연결이 성공합니다. 이제 인터넷에서 myVMWeb 가상 머신으로의 RDP 연결을 할 수 없습니다.
> 인터넷에서 모든 리소스로의 인바운드 트래픽은 기본적으로 거부됩니다.

3. Microsoft IIS를 **myVMWeb** 가상 머신에 설치하려면 **myVMWeb** 가상 머신에서 PowerShell을 실행하여 다음 명령을 입력하고 IIS서버를 활성화 합니다.

```
Install-WindowsFeature -name Web-Server -IncludeManageme
ntTools
```

4. IIS 설치가 완료되면 **myVMMgmt** VM의 원격 데스크탑 연결을 종료합니다.
5. 포털 검색 상자에서 *myVMWeb*을 검색합니다.
6. **myVMWeb**의 **개요** 페이지에서 VM의 **공용 IP 주소**를 복사합니다.

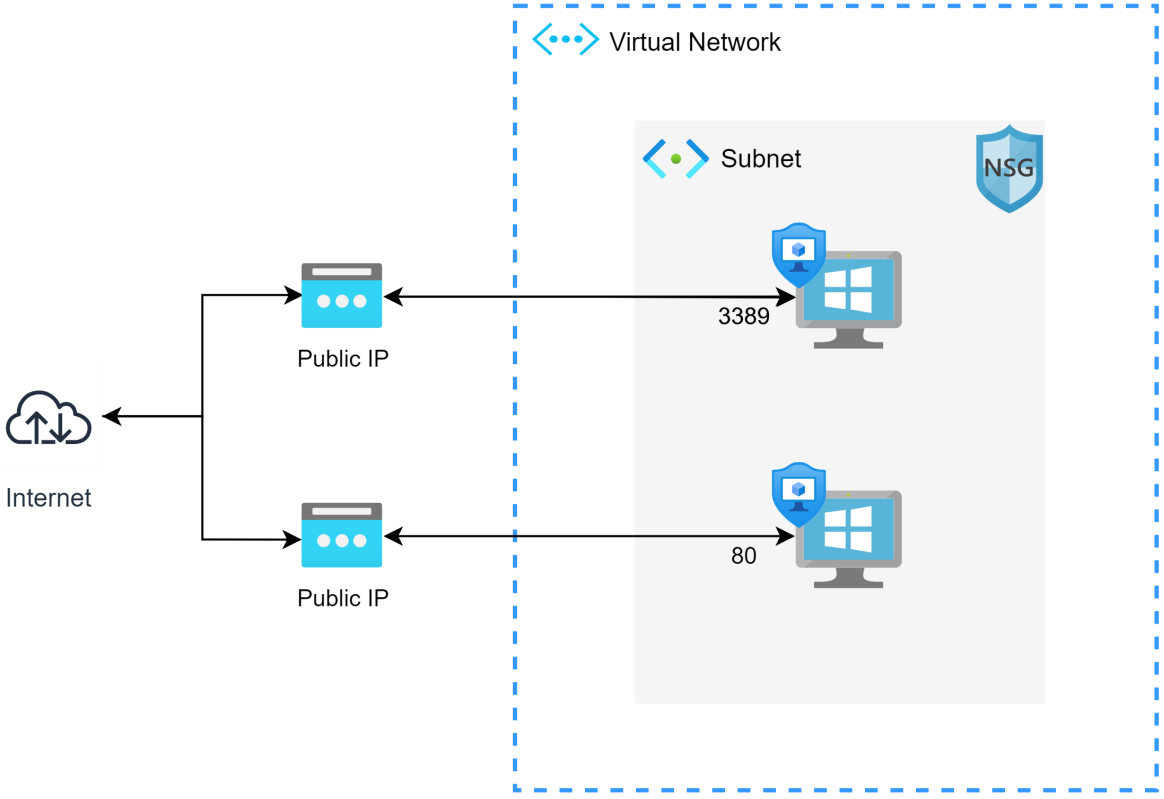


7. 인터넷에서 **myVMWeb** 웹 서버에 액세스할 수 있는지 확인하기 위해 컴퓨터에서 인터넷 브라우저에서 해당 주소로 이동합니다.

인터넷에서 **myAsgWebServers** 애플리케이션 보안 그룹으로의 인바운드 트래픽이 포트 80을 통해 허용되기 때문에 IIS 기본 페이지가 표시됩니다.

myVMWeb에 연결된 네트워크 인터페이스가 **myAsgWebServers** 애플리케이션 보안 그룹과 연결되어 연결을 허용합니다.

리소스 그룹에 생성된 리소스 확인



네트워크 보안 그룹은 1개이며 서브넷과 연결되어 있어 가상머신 모두다 설정이 적용됩니다. 애플리케이션 보안 그룹이 각 가상머신과 연결되어 있으므로 네트워크 보안 그룹의 설정 중 애플리케이션 보안 그룹이 연결된 설정만 각각 적용됩니다.

리소스 정리

네트워크 보안 그룹(NSG)을 통해 네트워크 트래픽 필터링 (원본)