

Lab24. 네트워크 트래픽 보안

1. 목적

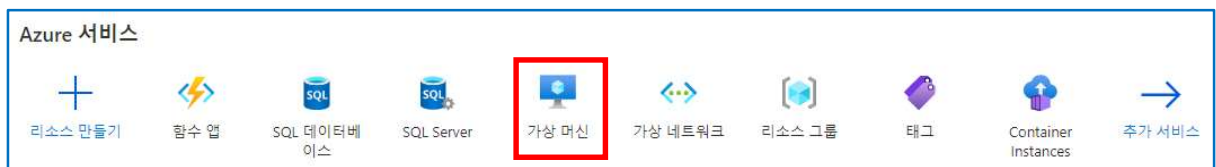
이번 실습에서는 네트워크 보안 그룹을 구성한다.

2. 사전 준비물

- Azure 체험 계정

3. 가상 머신 생성하기

A. **Azure Portal**에 로그인한다. **[Azure 서비스]** 섹션에서 **[가상 머신]**을 선택한다.



B. **[가상 머신]** 페이지에서 **[+만들기]** > **[가상 머신]**을 선택한다.



C. **[가상 머신 만들기]**에서 다음 각각의 값을 설정하고, 나머지 값은 기본값 그대로 놓는다.

- ① 구독 : 현재 계정의 구독
- ② 리소스 그룹 : [새로 만들기] > [myRGSecure]
- ③ 가상 머신 이름 : SimpleWinVM
- ④ 지역 : (Asia Pacific) 한국 중부
- ⑤ 이미지 : Windows Server 2019 Datacenter – Gen1

가상 머신 만들기 ...

[기본 사항](#) [디스크](#) [네트워킹](#) [관리](#) [고급](#) [태그](#) [검토 + 만들기](#)

Linux 또는 Windows를 실행하는 가상 머신을 만듭니다. Azure Marketplace에서 이미지를 선택하거나 고유한 사용자 지정 이미지를 사용합니다. [기본] 탭을 완료하고 [검토 + 만들기]하여 기본 매개 변수로 가상 머신을 프로비전하거나, 전체 사용자 지정에 대해 각 탭을 검토합니다. [자세한 정보](#)

프로젝트 정보

배포된 리소스와 비용을 관리할 구독을 선택합니다. 폴더 같은 리소스 그룹을 사용하여 모든 리소스를 정리 및 관리합니다.

구독 * ① MSDN 플랫폼 구독

리소스 그룹 * ① (신규) myRGSecure
[새로 만들기](#)

인스턴스 정보

가상 머신 이름 * ① SimpleWinVM

지역 * ① (Asia Pacific) 한국 중부

가용성 옵션 ① 인프라 중복이 필요하지 않습니다.

이미지 * ① Windows Server 2019 Datacenter - Gen1
[모든 이미지 보기](#)

⑥ 크기 : Standard_D2s_v3 – 2 vcpu, 8 GiB 메모리

⑦ 사용자 이름 : azureuser

⑧ 암호 / 암호 확인 : P@\$W0rd1234

⑨ 공용 인바운드 포트 : 없음.

크기 * ① Standard_D2s_v3 - 2 vcpu, 8 GiB 메모리 (₩100,982/월)
[모든 크기 보기](#)

관리자 계정

사용자 이름 * ① azureuser

암호 * ① *****

암호 확인 * ① *****

인바운드 포트 규칙

공용 인터넷에서 액세스할 수 있는 가상 머신 네트워크 포트를 선택하세요. [네트워킹] 탭에서 더 제한되거나 세분화된 네트워크 액세스를 지정할 수 있습니다.

공용 인바운드 포트 * ① ☒ 없음
☐ 선택한 포트 허용

인바운드 포트 선택 하나 이상의 포트 선택

i 인터넷의 모든 트래픽이 기본적으로 차단됩니다. [VM] > [네트워킹] 페이지에서 인바운드 포트 규칙을 변경할 수 있습니다.

D. [네트워킹] 탭을 클릭한다. 다음의 값만 설정하고, 나머지 값은 기본값 그대로 사용한다.

① NIC 네트워크 보안 그룹 : 없음

기본 사항 디스크 **네트워킹** 관리 고급 태그 검토 + 만들기

NIC(네트워크 인터페이스 카드) 설정을 구성하여 가상 머신에 대한 네트워크 연결을 정의합니다. 보안 그룹 규칙을 사용하여 포트, 인바운드 및 아웃바운드 연결을 제어하거나 기존 부하 분산 솔루션 뒤에 배치할 수 있습니다. [자세한 정보](#)

네트워크 인터페이스

가상 머신을 만들면 네트워크 인터페이스가 만들어집니다.

가상 네트워크 * ① (새로 만드는 중) myRGSecure-vnet
[새로 만들기](#)

서브넷 * ① (새로 만드는 중) default(10.0.0.0/24)
[새로 만들기](#)

공용 IP ① (새로 만드는 중) SimpleWinVM-ip
[새로 만들기](#)

NIC 네트워크 보안 그룹 ① ☒ 없음
☐ 기본
☐ 고급

E. [관리] 탭으로 이동하여 다음의 값을 설정하고 [검토 + 만들기]를 클릭한다.

① 부트 진단 : 사용 안 함

기본 사항 디스크 네트워크 **관리** 고급 태그 검토 + 만들기

VM에 대한 모니터링 및 관리 옵션을 구성합니다.

Azure Security Center

Azure Security Center는 하이브리드 클라우드 워크로드에서 통합 보안 관리 및 지능형 위협 방지 기능을 제공합니다. [자세한 정보](#)

구독은 Azure Security Center 기본 플랜으로 보호됩니다.

모니터링

부트 진단 ① ☐ 관리형 스토리지 계정으로 사용하도록 설정(권장)
☐ 사용자 지정 스토리지 계정으로 사용하도록 설정
☒ 사용 안 함

F. [유효성 검사 통과] 확인이 되면, [만들기]를 클릭한다.

가상 머신 만들기 ...

☒ 유효성 검사 통과

기본 사항 디스크 네트워크 관리 고급 태그 **검토 + 만들기**

제품 정보

표준 D2s v3 구독 크레딧 적용 ①
Microsoft Windows 138.3320KRW/시간
[사용 약관](#) | [개인 정보 취급 방침](#) [다른 VM 크기에 대한 가격 책정](#)

사용 약관

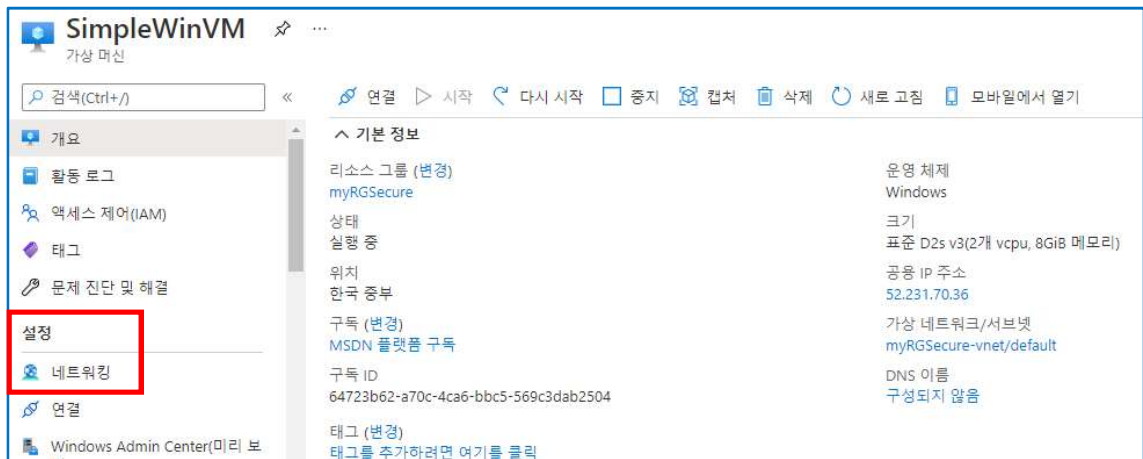
"만들기"를(를) 클릭함으로써 본인은 (a) 위의 해당 Marketplace 제품과 관련된 약관 및 개인정보처리방침에 동의하고, (b) Microsoft가 현재 결제 방법으로 제품과 관련된 요금을 내 Azure 구독과 동일한 대금 청구 주기로 청구하도록 권한을 부여하는 데 동의합니다. 또한 (c) Microsoft가 지원, 청구 및 기타 거래 목적으로 내 연락처 정보, 트랜잭션 정보 및 사용량 정보를 제품 공급자와 공유할 수 있다는 데 동의합니다. Microsoft는 타사 제품에 대한 권리를 제공하지 않습니다. 자세한 내용은 [Azure Marketplace 사용 약관](#)을 참조하세요.

만들기 < 이전 다음 > 자동화에 대한 템플릿 다운로드

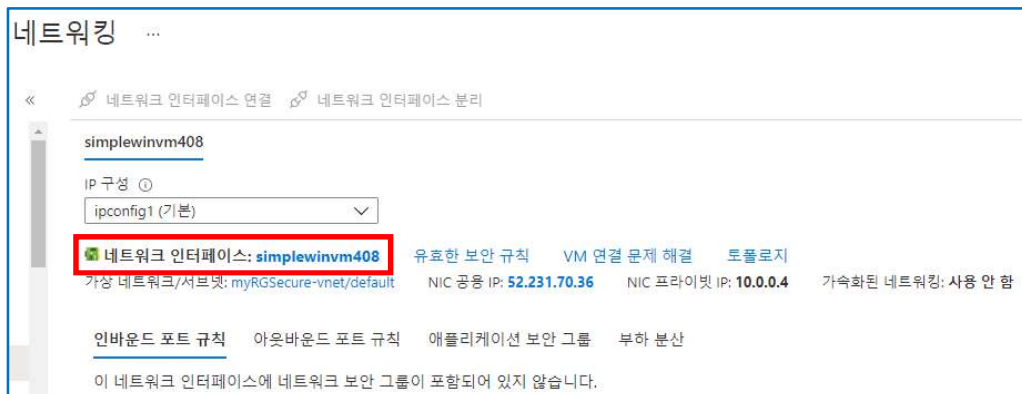
G. [배포가 완료됨]을 확인하고, [리소스로 이동]을 클릭한다.



H. 방금 생성한 SimpleWinVM 블레이드의 [개요]페이지에서, 좌측 서비스 메뉴 중 [네트워킹]를 선택한다.

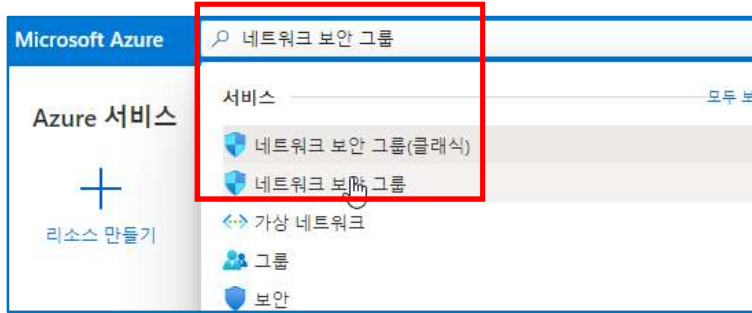


I. [네트워킹] 페이지에서 [인바운드 포트 규칙] 탭을 검토하고, 가상 머신의 [네트워크 인터페이스]나 네트워크 인터페이스가 연결된 [서브넷]과 연관된 [네트워크 보안 그룹]이 있는지 확인합니다.

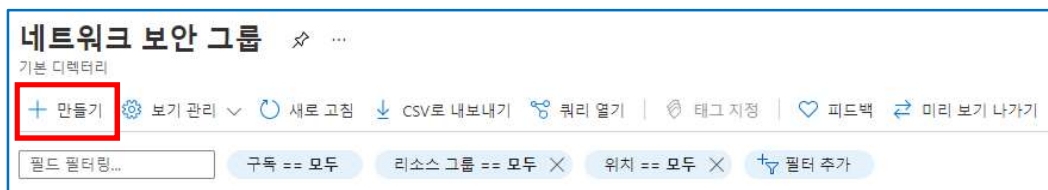


4. 네트워크 보안 그룹 생성하기

A. **Azure portal**에서 **전역 검색 상자**에 **네트워크 보안 그룹**으로 검색하여 선택한다.



B. **[네트워크 보안 그룹]** 페이지에서 **[+만들기]**를 클릭한다.



C. **[네트워크 보안 그룹 만들기]** 창에서 다음의 각각의 값을 설정한다. 나머지는 기본값 그대로 사용한다. 그리고 나서 **[검토 + 만들기]**를 클릭한다.

- ① 구독 : 현재 계정의 구독
- ② 리소스 그룹 : myRGSecure
- ③ 이름 : myNSGSecure
- ④ 지역 : (Asia Pacific) 한국 중부

D. [유효성 검사 통과] 확인 후, [만들기]를 클릭한다.

네트워크 보안 그룹 만들기 ...

유효성 검사 통과

기본 사항 태그 검토 + 만들기

기본 사항

구독	MSDN 플랫폼 구독
리소스 그룹	myRGSecure
지역	한국 중부
이름	myNSGSecure

태그

만들기 < 이전 다음 > 자동화에 대한 템플릿 다운로드

E. [배포가 완료됨]을 확인 후, [리소스로 이동]을 클릭한다.

배포가 완료됨

배포 이름: Microsoft.Network.SecurityGroup-20210723005347 시작 시간: 2021. 7. 23. 오전 12:58:30
구독: MSDN 플랫폼 구독 상관 관계 ID: c2ff8abc-152e-4a81-9089-66ec6c6823e3
리소스 그룹: myRGSecure

배포 정보 (다운로드)

다음 단계

리소스로 이동

F. [myNSGSecure] 블레이드에서 좌측 서비스 메뉴 중 [설정] > [네트워크 인터페이스]를 클릭한다.

myNSGSecure 네트워크 보안 그룹

검색(Ctrl+F)

이동 삭제 새로 고침

개요

- 활동 로그
- 액세스 제어(IAM)
- 태그
- 문제 진단 및 해결
- 설정
- 인바운드 보안 규칙
- 아웃바운드 보안 규칙
- 네트워크 인터페이스
- 서브넷

기본 정보

리소스 그룹 (변경)	사용자 지정 보안 규칙
myRGSecure	0 인바운드, 0 아웃바운드
위치	연결된 대상
한국 중부	0개 서버넷, 0개 네트워크 인터페이스
구독 (변경)	
MSDN 플랫폼 구독	
구독 ID	
64723b62-a70c-4ca6-bbc5-569c3dab2504	
태그 (변경)	
태그를 추가하려면 여기를 클릭	

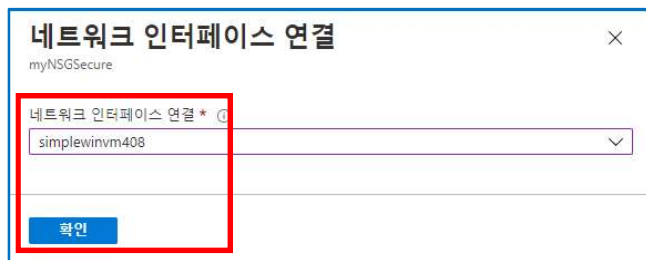
이름으로 필터링

포트 == 모두 프로토콜 == 모두 소스 == 모두 대상 주소 == 모두 작업 == 모두

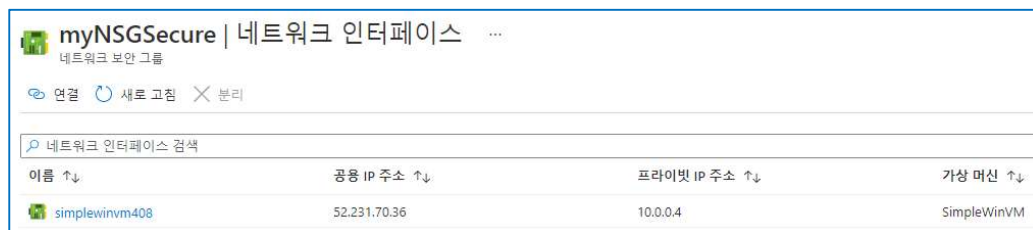
G. [네트워크 인터페이스] 페이지에서 [연결]을 클릭한다.



H. [네트워크 인터페이스 연결] 창에서 [네트워크 인터페이스 연결] 목록에서 이전 작업(3-1)에서 확인한 네트워크 인터페이스를 선택한다. 그리고 나서 [확인] 버튼을 클릭한다.

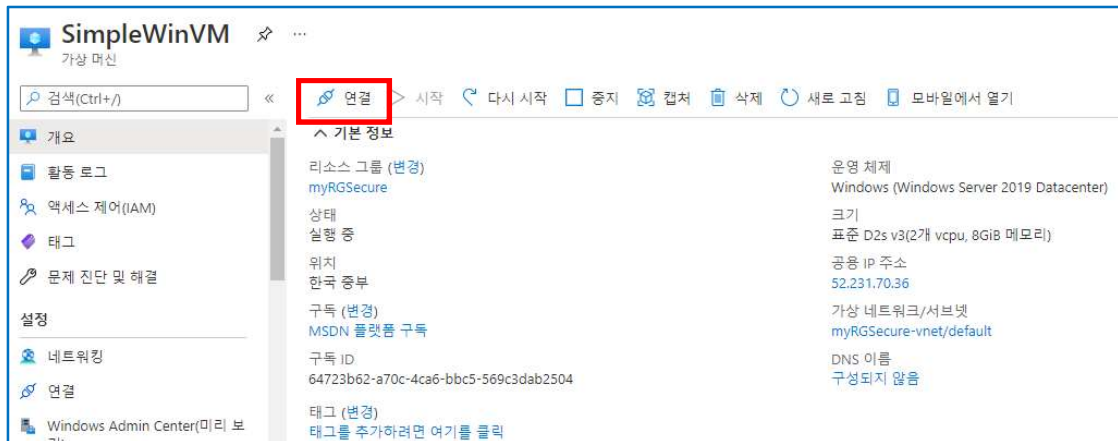


I. 결과는 아래 그림과 같다.



5. RDP를 허용하는 인바운드 보안 포트 규칙 구성하기

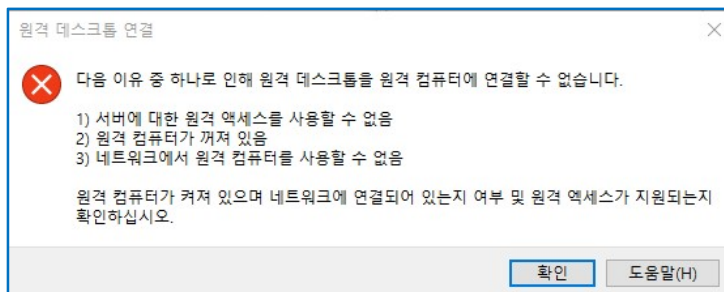
- A. **Azure Portal**에서 가상 머신 **SimpleWinVM** 블레이드로 이동한다. 명령바에서 **[연결] > [RDP]**을 선택한다.



- B. **[RDP 파일 다운로드]**를 클릭하여 연결을 시도한다.



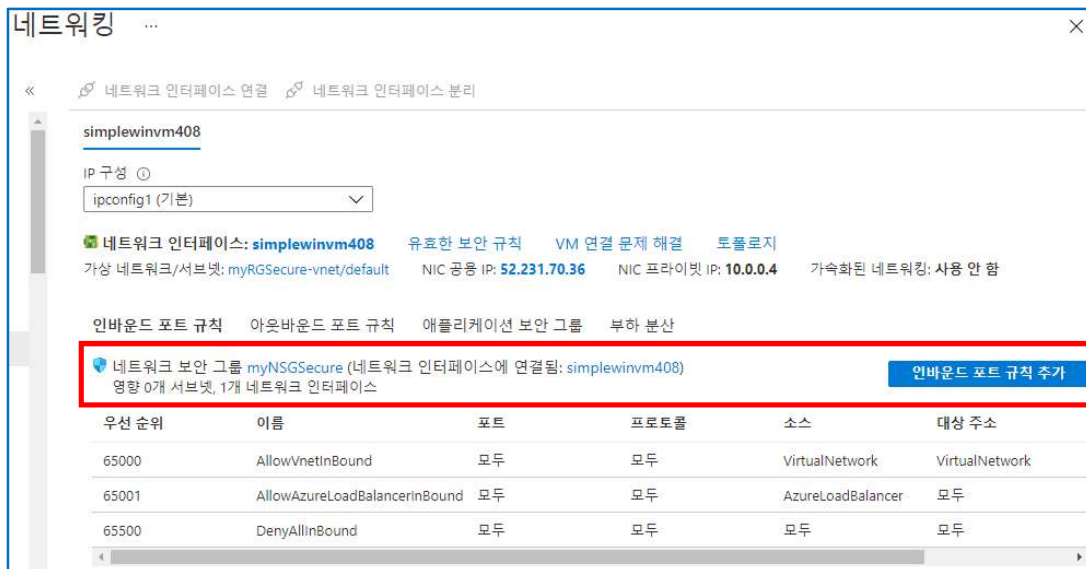
- C. 기본적으로 **네트워크 보안 그룹**은 RDP를 허용하지 않는다. 오류 창을 닫는다.



- D. 다시 **SimpleWinVM** 블레이드의 좌측 서비스 메뉴 중 **[설정] > [네트워킹]**을 선택한다.



- E. **myNSGSecure(네트워크 인터페이스에 연결됨: simplewinvm408)** 네트워크 보안 그룹의 인바운드 규칙이 가상 네트워크와 부하 분산 장치 프로브내의 트래픽을 제외한 모든 인바운드 트래픽을 거부하는 것을 확인한다. **[인바운드 포트 규칙 추가]** 버튼을 클릭한다.



- F. **[인바운드 보안 규칙 추가]**창에서 다음의 각 값을 설정하고, 나머지는 기본값을 그대로 사용하기로 하고 **[추가]** 버튼을 클릭한다.

- ① 서비스 : RDP
- ② 대상 포트 범위 : 3389
- ③ 프로토콜 : TCP
- ④ 작업 : 허용
- ⑤ 우선 순위 : 300
- ⑥ 이름 : AllowRDP

인바운드 보안 규칙 추가 myNSGSecure

소스 ①
Any

원본 포트 범위 * ①
*

대상 주소 ①
Any

서비스 ①
RDP

대상 포트 범위 ①
3389

프로토콜
☐ Any
☒ TCP
☐ UDP
☐ ICMP

작업
☒ 허용
☐ 거부

우선 순위 * ①
300

이름 *
AllowRDP

추가 취소

G. 추가한 **AllowRDP**를 확인한다.

인바운드 포트 규칙 아웃바운드 포트 규칙 애플리케이션 보안 그룹 부하 분산

네트워크 보안 그룹 myNSGSecure (네트워크 인터페이스에 연결됨: simplewinvm408)
영향 0개 서버넷, 1개 네트워크 인터페이스

인바운드 포트 규칙 추가

우선 순위	이름	포트	프로토콜	소스	대상 주소
300	AllowRDP	3389	TCP	모두	모두
65000	AllowVnetInBound	모두	모두	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	모두	모두	AzureLoadBalancer	모두
65500	DenyAllInBound	모두	모두	모두	모두

H. 다시 **SimpleWinVM** 가상 머신과 연결을 시도한다. 이번에는 성공해야 한다.

Windows 보안

사용자 자격 증명 입력

이 자격 증명은 52.231.70.36에 연결할 때 사용됩니다.

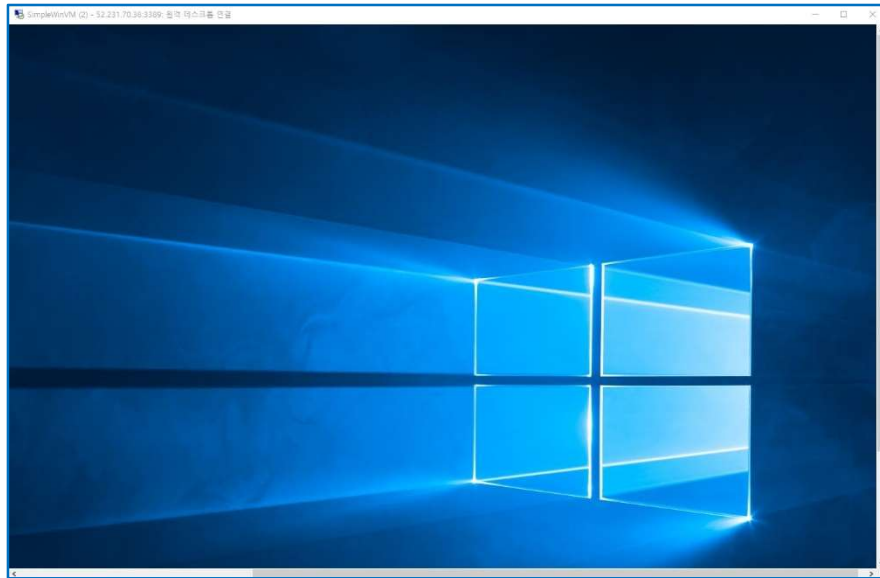
azureuser

●●●●●●●●●●●●●●●●

☐ 기억

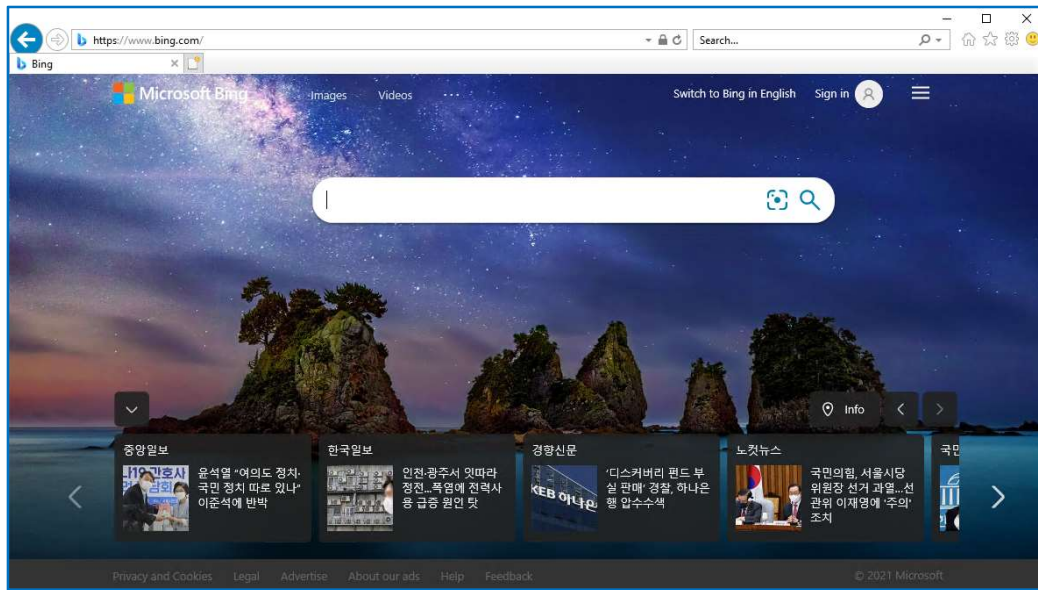
확인 취소

1. 가상 머신과 잘 연결되었다.



6. 인터넷 액세스를 거부하는 아웃바운드 보안 포트 규칙 구성하기

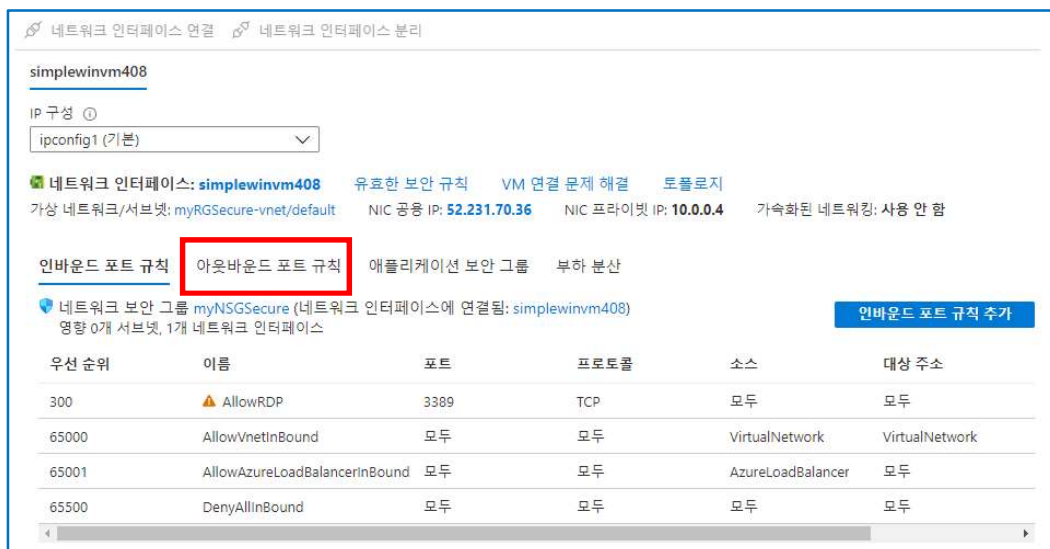
- A. 가상 머신에서 **Internet Explorer**를 오픈한다. <https://www.bing.com>에 액세스할 수 있는지 확인한 뒤, **Internet Explorer**를 닫는다.



- B. Azure Portal에서 **SimpleWinVM** 가상 머신의 블레이드 페이지로 이동한다. 좌측 서비스 메뉴에서 **[설정] > [네트워킹]**을 선택한다.



- C. **[네트워킹]** 페이지에서 **[아웃바운드 포트 규칙]** 탭을 클릭한다.



- D. **AllowInternetOutbound**라는 규칙을 확인할 수 있다. 이 규칙은 기본 규칙이며 제거할 수 없다. [아웃바운드 포트 규칙 추가]를 클릭한다.


아아웃바운드 포트 규칙

네트워크 보안 그룹 myNSGSecure (네트워크 인터페이스에 연결됨: simplewinvm408)
영향 0개 서버넷, 1개 네트워크 인터페이스

우선 순위	이름	포트	프로토콜	소스	대상 주소
65000	AllowVnetOutBound	모두	모두	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	모두	모두	모두	Internet
65500	DenyAllOutBound	모두	모두	모두	모두

- E. 인터넷 트래픽을 거부할 더 높은 우선 순위의 새 아웃바운드 보안 규칙을 구성한다. 다음 각 각의 값을 설정하고 완료되면 **[추가]**를 클릭한다.

- ① 소스 : Any
- ② 대상 주소 : Service Tag
- ③ 대상 서비스 태그 : Internet
- ④ 대상 포트 범위 : *
- ⑤ 프로토콜 : TCP
- ⑥ 작업 : 거부
- ⑦ 우선 순위 : 4000
- ⑧ 이름 : DenyInternet



아웃바운드 보안 규칙 추가

myNSGSecure

소스 ⓘ

Any

원본 포트 범위 * ⓘ

*

대상 주소 ⓘ

Service Tag

대상 서비스 태그 ⓘ

Internet

서비스 ⓘ

Custom

대상 포트 범위 * ⓘ

*

프로토콜

☐ Any
 ☒ TCP
 ☐ UDP
 ☐ ICMP

작업

☐ 허용
 ☒ 거부

우선 순위 * ⓘ

4000

이름 *

DenyInternet

추가

취소

F. 방금 추가한 아웃바운드 포트 규칙을 확인할 수 있다.

아웃바운드 포트 규칙					
네트워크 보안 그룹 myNSGSecure (네트워크 인터페이스에 연결됨: simplewinvm408) 영향 0개 서버넷, 1개 네트워크 인터페이스					
아웃바운드 포트 규칙 추가					
우선 순위	이름	포트	프로토콜	소스	대상 주소
4000	DenyInternet	모두	TCP	모두	Internet
65000	AllowVnetOutBound	모두	모두	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	모두	모두	모두	Internet
65500	DenyAllOutBound	모두	모두	모두	모두

G. 다시 **SimpleWinVM** 원격 데스크톱으로 돌아간다. <https://www.microsoft.com>으로 웹 브라우저를 열고 연결을 시도한다. 페이지가 연결되지 않아야 한다.

