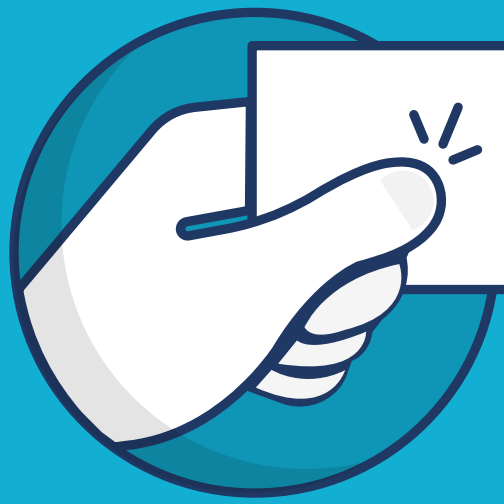
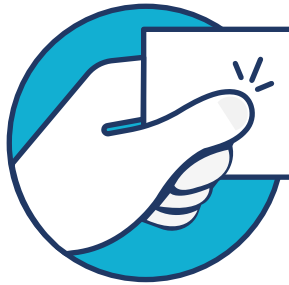


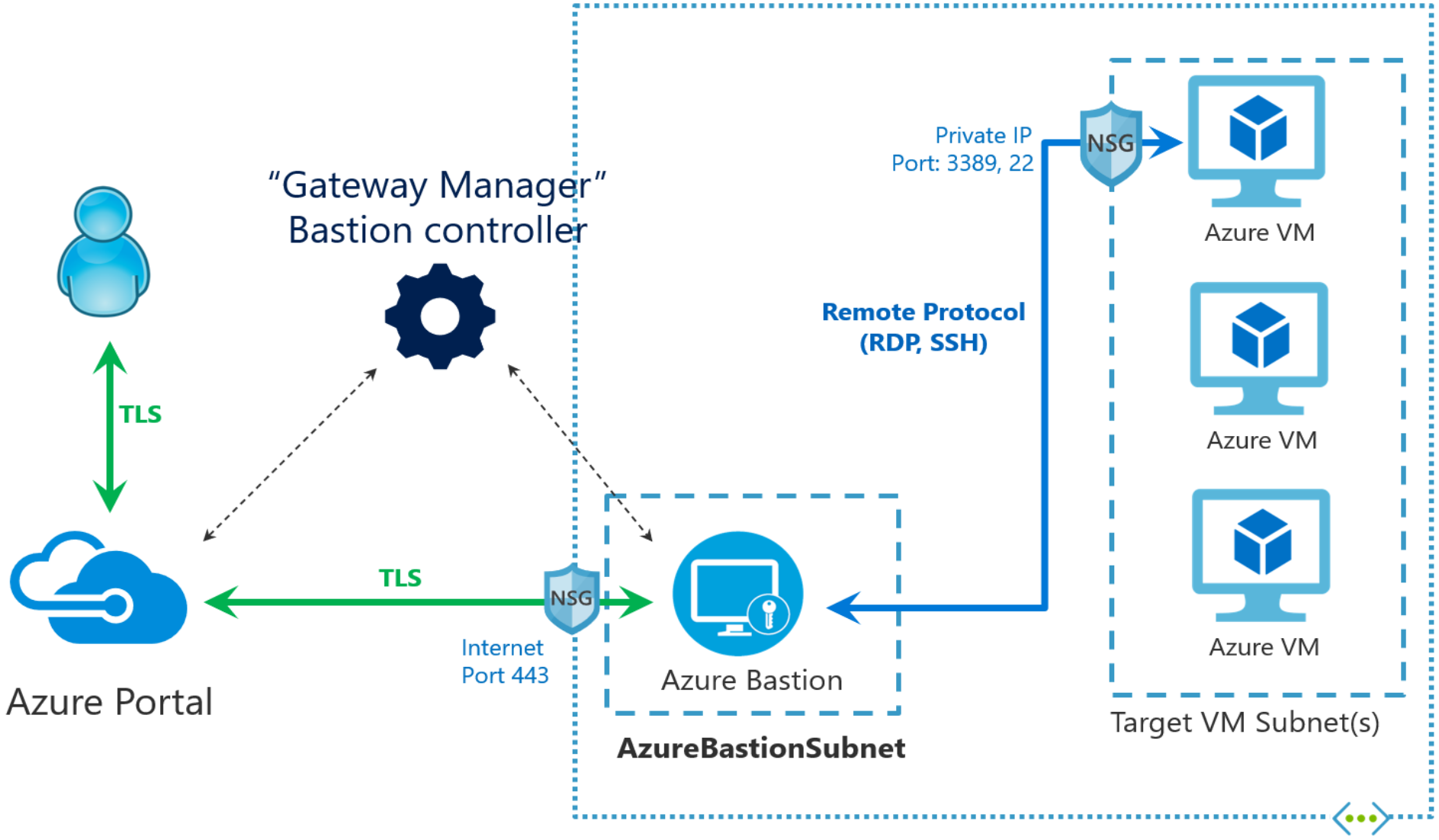
13장 핵심 인프라 보호



13장 개요

- 네트워크 보안 그룹의 개념과 옵션, 트래픽 제어 설정
- Azure 배스천 서비스의 개념과 동작 방식, 배포 및 설정
- Azure 스토리지 계정의 고급 보안 기능과 계층화된 보안 모델 구성

1. 네트워크 보안 그룹(NSG)



1. 네트워크 보안 그룹(NSG)

- 가상 네트워크의 리소스에 대한 인바운드와 아웃바운드 네트워크 트래픽을 허용하거나 거부하는 데 사용하는 가상 방화벽 역할의 보안계층

- 서브넷이나 네트워크 인터페이스에 적용

1. 네트워크 보안 그룹(NSG)

- 인바운드 기본 규칙 - 가상 네트워크와 Azure 부하 분산장치에서 들어오는 인바운드 트래픽을 제외한 모든 트래픽 거부
- 아웃바운드 기본 규칙 – 인터넷과 가상 네트워크에 대한 아웃바운드 트래픽만 허용하고 그 외는 모두 거부한다.

우선 순위 ↑↓	이름 ↑↓	포트 ↑↓	프로토콜 ↑↓	소스 ↑↓	대상 주소 ↑↓	작업 ↑↓
인바운드 보안 규칙						
65000	AllowVnetInBound	모두	모두	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	모두	모두	AzureLoadBalancer	모두	Allow
65500	DenyAllInBound	모두	모두	모두	모두	Deny
아웃바운드 보안 규칙						
65000	AllowVnetOutBound	모두	모두	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	모두	모두	모두	Internet	Allow
65500	DenyAllOutBound	모두	모두	모두	모두	Deny

1. 네트워크 보안 그룹(NSG)

- 보안 규칙

- 보안규칙에 일치하는 경우 트래픽을 허용하거나 거부할 수 있다.

- 네트워크 인터페이스

- 네트워크 인터페이스에 연결하면 가상 머신으로 들어오고 나가는 트래픽을 제어할 수 있다.

- 서브넷

- 네트워크 보안 그룹을 연결하면 해당 서브넷에 있는 모든 가상 머신으로의 트래픽 흐름을 제한할 수 있다.

1. 네트워크 보안 그룹(NSG)

가상네트워크

- Subnet1개

가상머신

- ubuntu
- 공용 ip O
- 인바운드 규칙 80prot
- 생성한 가상네트워크
- NGINX설치

NSG

- 가상네트워크
- subnet 연결

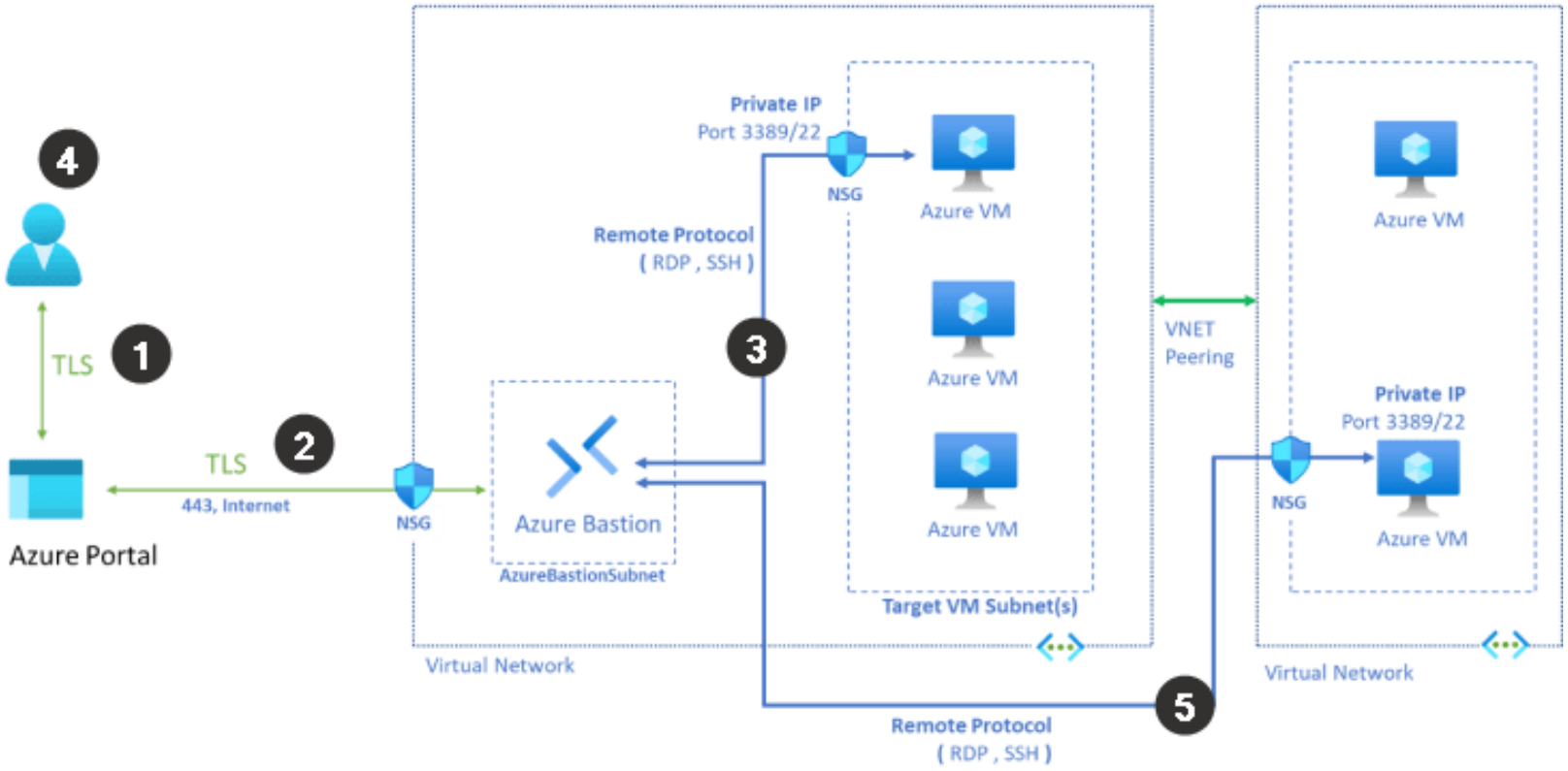
2. Bastion 서비스의 이점과 동작 방식

Bastion - TLS(전송 계층 보안)을 통해 Azure Portal에서 가상머신에 안전하고 간단하게 연결할 수 있게 해주는 기능

이점

- 개인 IP를 통해 가상머신에 연결하기 때문에 공인 IP가 필요하지 않음.
- 완전 관리형 PaaS이므로 별다른 보안이 더 필요없음.
- Azure Bastion 서브넷과 동일한 가상 네트워크에 있는 모든 VM에 연결할 수 있음.
- Bastion을 위한 별다른 프로그램이 필요 없음.

2. Bastion 서비스의 이점과 동작 방식



3. 스토리지 보호(NSG)

스토리지에 사용할 수 있는 고급 보안 기능
- 암호화
- 인증
- 보안 전송
- 디스크 암호화
- 공유 액세스 서명

계층화된 보안 모델
- 방화벽
- 가상 네트워크 선택

3. 스토리지 보호(NSG)

방화벽 및 가상 네트워크(무료)

특정 가상 네트워크의 서브넷에 추가한 서비스 엔드포인트를 통해 스토리지를 액세스 하도록 네트워크 규칙을 만들어 액세스를 제어하고 방화벽 정책을 통해 특정 인터넷 지점에서만 액세스를 허용

공유 액세스 서명(SAS)

스토리지 계정의 리소스에 대한 안전하고 위임된 권한을 제공. SAS를 사용하면 클라이언트가 데이터에 액세스하는 방법을 세부적으로 제어
특정 리소스에 대한 권한을 가진 클라이언트 애플리케이션에게만 접근 권한을 부여하고, 미리 정의된 기간 동안에만 그 권한을 유지하도록 허용

3. 스토리지 보호(NSG)

SAS

- 사용자 위임 SAS
클라이언트 응용 프로그램이나 서비스가 다른 사용자에게 리소스 액세스를 위임할 수 있도록 하는 메커니즘을 제공

- 서비스 SAS
Storage Account의 여러 서비스에 대한 권한을 부여합니다. 예를 들어 Blob, Queue, Table, File 서비스에 대한 권한을 함께 부여

- 계정 SAS
Storage Account 전체에 대한 권한을 부여합니다. 특정 서비스가 아닌 전체 Storage Account에 대한 액세스 권한을 제공하는 경우 사용

4. 덤프풀이

시험 AZ-104를 위한 연습 평가: Microsoft Azure 관리자

50개 중 25개 질문

파일 공유를 포함하는 Azure Storage 계정이 있습니다.

여러 사용자가 인터넷으로의 아웃바운드 트래픽을 제한하는 안전한 위치에서 작업합니다.

보안 위치에 있는 사용자가 SMB 프로토콜을 사용하여 Azure의 파일 공유에 액세스할 수 있는지 확인해야 합니다.

보안 위치에서 어떤 아웃바운드 포트를 허용해야 하나요?

- ◯ 80
- ◯ 443
- ◯ 445
- ◯ 5671

다음 > 답변 확인

4. 덤프풀이

- ○ 80
- ○ 443
- ○ 445

✓정답입니다.

- ◉ 5671

이 답은 틀렸습니다.

파일 공유에 액세스하려면 포트 445를 열어야 합니다. 포트 5671은 Microsoft Entra에 상태 정보를 보내는 데 사용됩니다. 최신 버전에서는 권장되지만 필수는 아닙니다. 포트 80은 TLS/SSL 인증서를 확인하기 위해 CRL(인증서 해지 목록)을 다운로드하는 데 사용됩니다. 포트 443은 AD DS를 Microsoft Entra와 동기화하는 등의 https 트래픽에 사용됩니다.

하이브리드 ID 필수 포트 및 프로토콜 - Azure - Microsoft Entra | Microsoft Learn

Azure Storage 보안 구성 - 학습 | Microsoft Learn

다음 > 답변 확인

4. 덤프풀이

RG1 및 RG2라는 두 개의 리소스 그룹이 포함된 Azure 구독이 있습니다.

RG1에는 다음 리소스가 포함됩니다.

- 미국 동부 Azure 지역에 있는 VNet1이라는 가상 네트워크
- 미국 서부 Azure 지역에 있는 NSG1이라는 NSG(네트워크 보안 그룹)

RG2에는 다음 리소스가 포함됩니다.

- 미국 동부 Azure 지역에 있는 VNet2라는 가상 네트워크
- 미국 서부 Azure 지역에 있는 VNet3이라는 가상 네트워크

NSG1을 적용해야 합니다.

NSG1을 적용할 수 있는 서브넷은 무엇인가요?

- ◯ 모든 가상 네트워크의 서브넷
- ◯ VNet1의 서브넷만
- ◯ VNet1 및 VNet2의 서브넷
- ◉ VNet3의 서브넷만

4. 덤프풀이

- ◯ 모든 가상 네트워크의 서브넷
- ◯ VNet1의 서브넷만
- ◯ VNet1 및 VNet2의 서브넷
- ◉ VNet3의 서브넷만

✓정답입니다.

NSG 및 NSG1이 미국 서부 지역에 있는 것과 동일한 지역에 있는 가상 네트워크의 서브넷에 NSG를 할당할 수 있습니다.

Azure 가상 네트워크 계획 | Microsoft Learn

네트워크 보안 그룹 구성 - 학습 | Microsoft Learn

4. 덤프풀이

NSG1이라는 NSG(네트워크 보안 그룹)가 포함된 Azure 구독이 있습니다.

다음 유형의 트래픽을 허용하도록 NSG1을 구성할 계획입니다.

- 원격 데스크톱 관리
- 보안 HTTPS

NSG1에서 어떤 두 포트를 허용해야 하나요? 각 정답은 해답의 일부를 나타냅니다.

- [ ] 80
- [ ] 25
- [ ] 443
- [ ] 587
- [ ] 3389

4. 덤프풀이

- [ ] 80
- [ ] 25
- [ ] 443

✓정답입니다.

- [x] 587

이 답은 틀렸습니다.

- [ ] 3389

✓정답입니다.

포트 443을 열어 보안 HTTPS 트래픽, 원격 데스크톱용 포트 3389, 인증된 SMTP 릴레이를 사용하여 아웃바운드 이메일을 보내려면 587을 열어야 합니다. 포트 80은 보안되지 않은 트래픽에 사용됩니다. 포트 25는 메일 트래픽에 사용됩니다.

잠금으로 Azure 리소스 보호 - Azure Resource Manager | Microsoft Learn

네트워크 보안 그룹 구성 - 학습 | Microsoft Learn

4. 덤프풀이

NSG1이라는 NSG(네트워크 보안 그룹)에 할당된 VM1이라는 가상 머신이 있습니다.

NSG1에는 다음과 같은 아웃바운드 보안 규칙이 있습니다.

Rule1:

- 우선 순위: 900
- 이름: BlockInternet
- 포트 = 80
- 프로토콜: TCP
- 원본: 모두
- 대상: 모두
- 작업: Block

Rule2:

- 우선 순위: 1000
- 이름: AllowInternet
- 포트 = 80
- 프로토콜: TCP
- 원본: 모두
- 대상: 모두
- 작업: 허용

포트 80에서 VM1에 대한 인터넷 액세스가 허용되는지 확인해야 합니다.

어떻게 해야 합니까?

◯ Rule2의 동작을 변경합니다.

◯ Rule1의 이름을 변경합니다.

◯ Rule2의 우선 순위를 변경합니다.

◯ 규칙 2의 원본을 변경합니다.

4. 덤프풀이

- ○ Rule2의 동작을 변경합니다.
- ○ Rule1의 이름을 변경합니다.
- ◉ Rule2의 우선 순위를 변경합니다.

  ✓정답입니다.
- ○ 규칙 2의 원본을 변경합니다.

Rule1의 우선 순위가 높으므로 작업이 차단됩니다. Rule2의 우선 순위를 높이거나, Rule1의 우선 순위를 줄이거나, Rule1의 작업을 변경하여 목표를 달성할 수 있습니다.

Azure 네트워크 보안 그룹 개요 | Microsoft Docs

네트워크 보안 그룹 구성 - 학습 | Microsoft Learn

4. 덤프풀이

Windows Server를 실행하는 여러 Azure 가상 머신을 만듭니다.

인터넷을 통해 RDP 포트를 노출하지 않고 가상 머신에 연결해야 합니다.

어떤 Azure 서비스를 배포해야 하나요?

- Azure Bastion
- Azure Front Door
- Azure Network Watcher
- Azure Virtual Desktop

4. 덤프풀이

- [x] Azure Bastion

✓정답입니다.

- [ ] Azure Front Door
- [ ] Azure Network Watcher
- [ ] Azure Virtual Desktop

Azure Bastion은 RDP 및 SSH 포트를 노출하지 않고 브라우저를 사용하여 가상 머신에 연결할 수 있는 서비스입니다. Azure Monitor를 사용하면 애플리케이션 및 서비스의 가용성과 성능을 최대화할 수 있습니다. Azure Network Watcher는 Azure 가상 네트워크의 리소스를 모니터링 및 진단하고 메트릭을 보고 그에 대한 로그를 활성화 또는 비활성화하는 도구를 제공합니다. 원격 데스크톱은 인터넷에서 서버에 연결할 RDP 포트를 노출하는 운영 체제의 기능입니다.

Azure Bastion 정보 | Microsoft Learn
가상 네트워크 구성 - 학습 | Microsoft Learn

4. 덤프풀이

4개의 서브넷을 포함하는 Azure 가상 네트워크가 있습니다. 각 서브넷에는 10개의 가상 머신이 포함됩니다.

TCP 포트 8080을 통해 각 서브넷의 두 가상 머신으로 인바운드 트래픽을 허용하는 NSG(네트워크 보안 그룹)를 구성할 계획입니다. NSG는 각 서브넷에 연결됩니다.

가능한 가장 적은 수의 NSG 규칙을 사용하여 인바운드 액세스를 구성하는 솔루션을 권장해야 합니다.

NSG에서 대상으로 무엇을 사용해야 하나요?

- (●) 애플리케이션 보안 그룹
- ( ) 서비스 태그
- ( ) 가상 머신의 서브넷

4. 덤프풀이

- ○ 애플리케이션 보안 그룹

✓정답입니다.

- ◉ 서비스 태그

이 답은 틀렸습니다.

- ○ 가상 머신의 서브넷

애플리케이션 보안 그룹을 사용하면 여러 가상 머신의 네트워크 인터페이스를 그룹화한 다음, NSG 규칙에서 그룹을 원본 또는 대상으로 사용할 수 있습니다. 네트워크 인터페이스는 동일한 가상 네트워크에 있어야 합니다.
각 가상 머신의 IP 주소를 대상으로 사용할 수 있지만 각 가상 머신에 대한 규칙을 만들어야 합니다.
서브넷을 사용하려면 네 가지 규칙이 필요하며 해당 서브넷의 모든 가상 머신에 대한 트래픽도 허용합니다.
서비스 태그는 Azure App Service 또는 Azure Backup과 같은 특정 Azure 서비스에 대한 것입니다.
Azure 애플리케이션 보안 그룹 개요 | Microsoft Learn
네트워크 보안 그룹 구성 - 학습 | Microsoft Learn