Microsoft Cloud Workshop

Azure IaaS 101

Hands-on lab step-by-step

Lab 6

Aug 2018

Moonsun Lee (CSA)

Contents

IaaS 101 hands-on lab step-by-step **1**

목표 1

Lab 구성 2

요구사항 3

Lab 6: P2S(지점 및 사이트간) VPN 구성하기 4

Step 1: 가상 네트워크 게이트웨이 생성 4

Step 2: 서명된 인증서 생성 (Root / Client) 및 Azure 에 등록 8

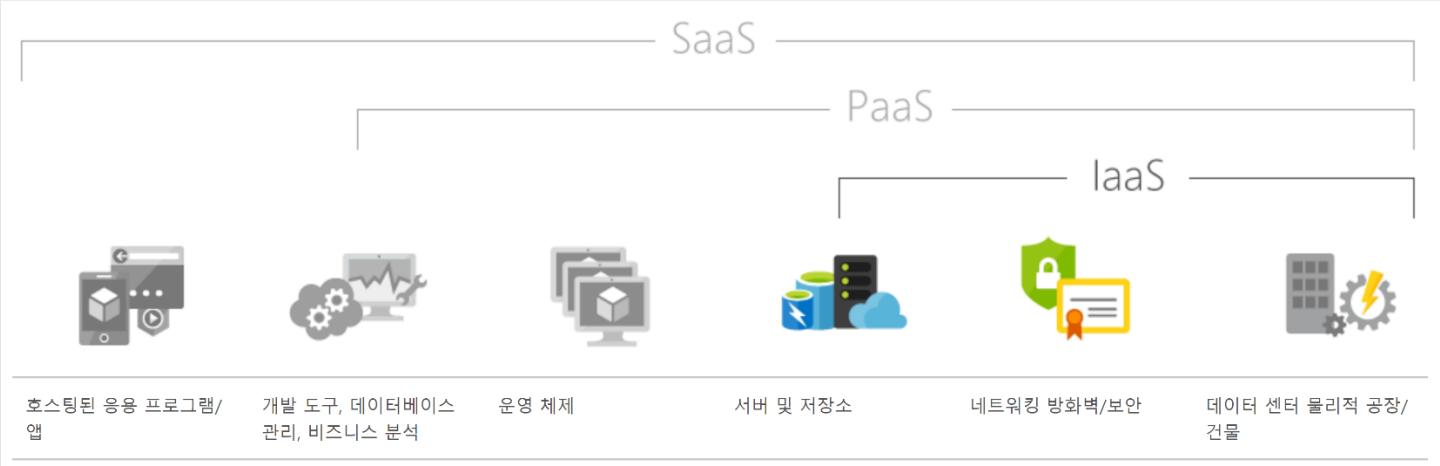
Step 3: 로컬머신에 Azure VPN 클라이언트 설치 19

IaaS 101 hands-on lab step-by-step

목표

IaaS(Infrastructure as a Service)는 인터넷을 통해 프로비전 및 관리되는 즉각적인 컴퓨팅 인프라입니다. 수요에 따라 빠르게 강화/규모 축소할 수 있으며 사용한 양만큼만 비용을 지급하면 됩니다.

IaaS 를 사용할 경우 자체 물리적 서버와 기타 데이터 센터 인프라를 구입하고 관리하는 데 따른 비용과 복잡성이 없어집니다. 각 리소스는 별도의 서비스 구성 요소로 제공되며, 특정 리소스를 필요한 동안에만 대여하면 됩니다. 클라우드 컴퓨팅 서비스 공급자는 인프라를 관리하는 반면, 사용자는 자체 소프트웨어(운영 체제, 미들웨어 및 응용 프로그램)를 구매, 설치, 구성 및 관리합니다.



해당 실습은 Azure IaaS(Infrastructure as a Service)를 처음 접해보는 엔지니어를 대상으로 작성되었으며, 실습을 통하여 아래 나열된 Azure 의 IaaS 의 주요 서비스들을 직접 만들어보며 이해할 수 있도록 구성되어 있습니다.

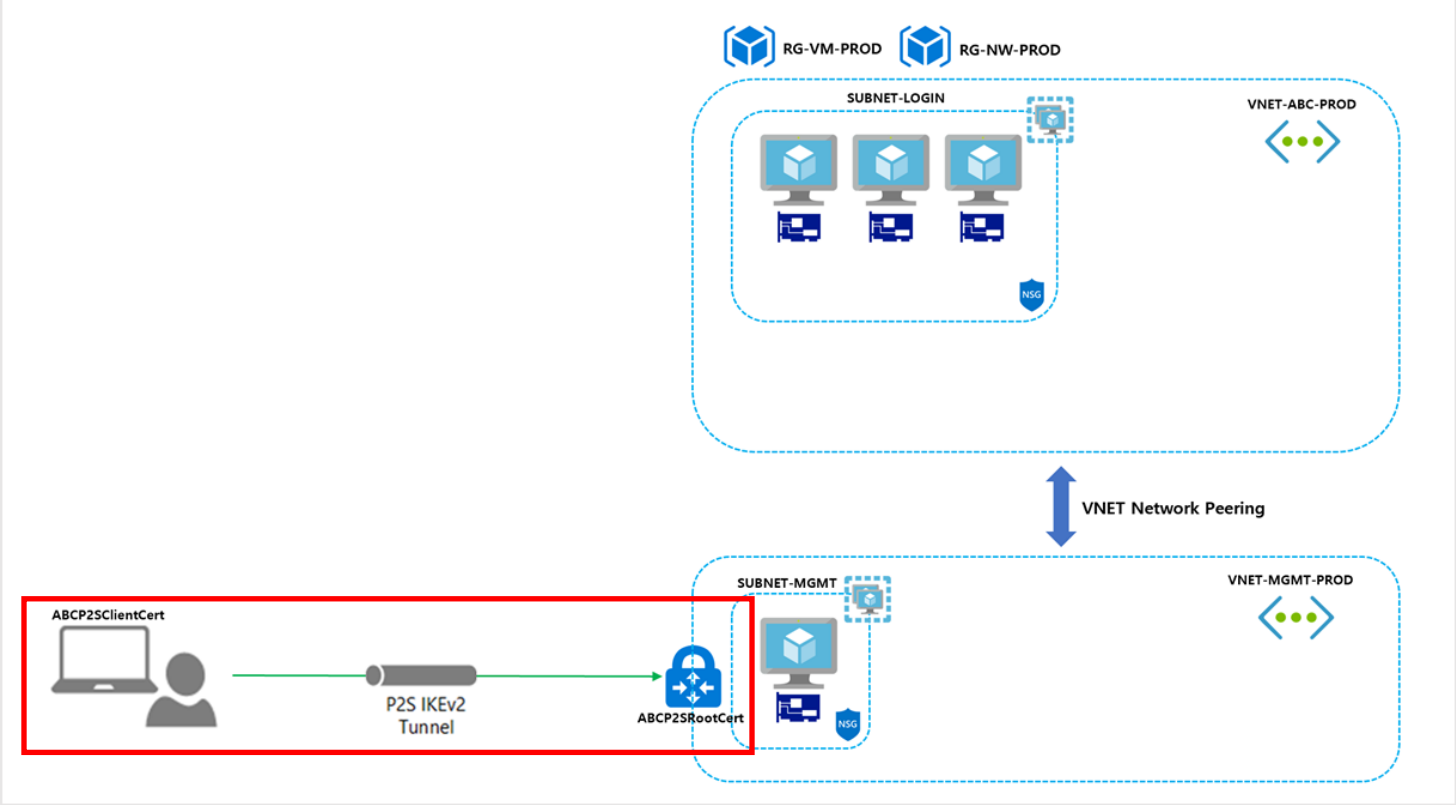
- Azure 가상머신
- Azure 가상네트워크 (서브넷 / 피어링 / 보안)
- Azure VPN 서비스
- Azure 스토리지

Lab 구성

Duration: 45 minutes

Point to Site(P2S, 지점 및 사이트 간) VPN 게이트웨이 연결을 사용하면 개별 클라이언트 컴퓨터에서 가상 네트워크에 대한 안전한 연결을 만들 수 있습니다.

P2S VPN 연결은 클라이언트 컴퓨터에서 시작하여 설정됩니다. 이 솔루션은 집 또는 회의실과 같은 원격 위치에서 Azure VNet 에 연결하려는 재택 근무자에게 유용합니다. 또한 P2S VPN 은 가상 네트워크에 연결해야 하는 클라이언트가 몇 개만 있는 경우 Site to Site(S2S, 지점 및 지점) VPN 대신 사용할 수 있는 유용한 솔루션입니다.



이번 실습에서는, 아래 단계들을 통하여 **VNET-ABC-MGMT** 로의 P2S VPN 생성 실습을 진행하며 Windows 10 로컬머신 기준으로 작성되었습니다.

- 게이트웨이 서브넷 생성
- 가상 네트워크 게이트웨이(Virtual Network Gateway) 생성
- 인증서 생성(Root/Client)
- Azure 내 인증서(Root) 등록
- 인증서 설치 및 Azure 로의 접속

요구사항

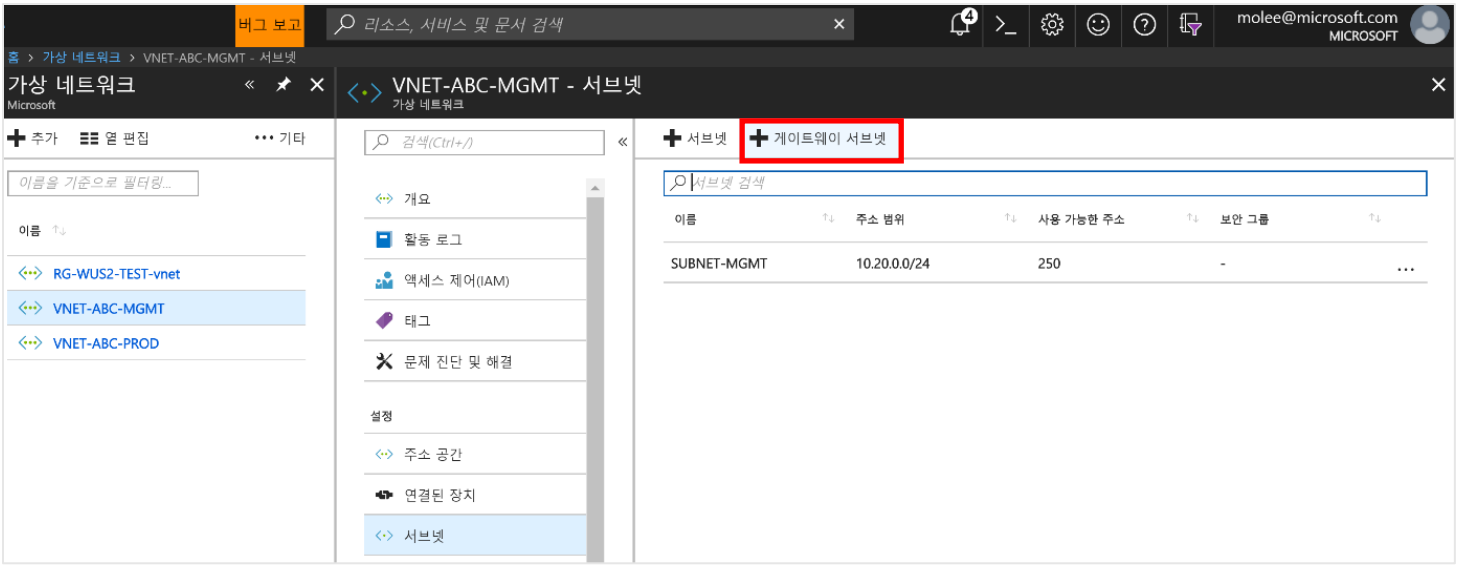
- Microsoft Azure subscription
- Local machine
- Lab 1 – 5 실습

Lab 6: P2S(지점 및 사이트간) VPN 구성하기

Step 1: 가상 네트워크 게이트웨이 생성

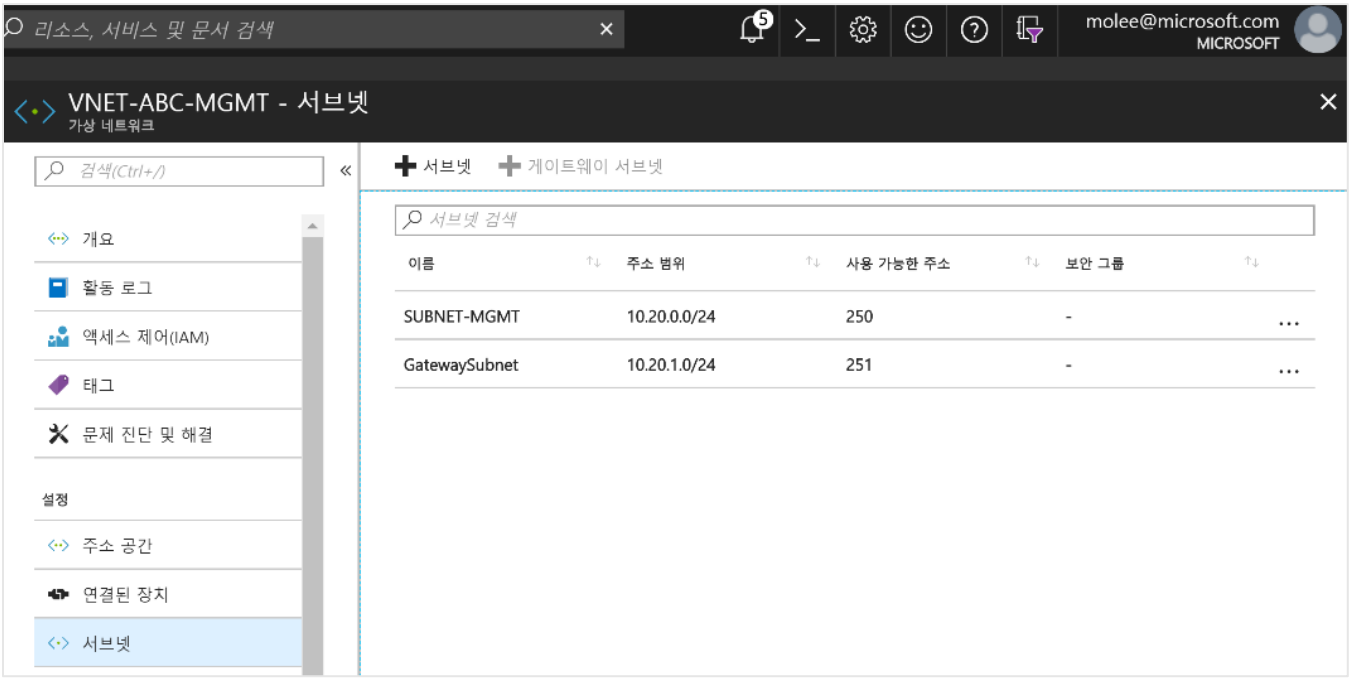
가상 네트워크를 게이트웨이에 연결하기 전에 먼저 연결하려는 가상 네트워크에 대한 게이트웨이 서브넷을 만들어야 합니다. 게이트웨이 서비스는 게이트웨이 서브넷에 지정된 IP 주소를 사용합니다. 향후 추가적인 구성 요구 사항을 수용하기에 충분한 IP 주소를 제공하도록 가능하면 /28 또는 /27 CIDR 블록을 사용하여 게이트웨이 서브넷을 만듭니다.

1. VPN 을 설정하려는 **VNET-ABC-MGMT** 가상 네트워크 페이지로 이동한 뒤, 서브넷 버튼을 클릭하여 가상네트워크-서브넷 페이지로 이동합니다. 서브넷 페이지에서 "+게이트웨이 서브넷" 버튼을 클릭하여 서브넷 추가 페이지를 엽니다.



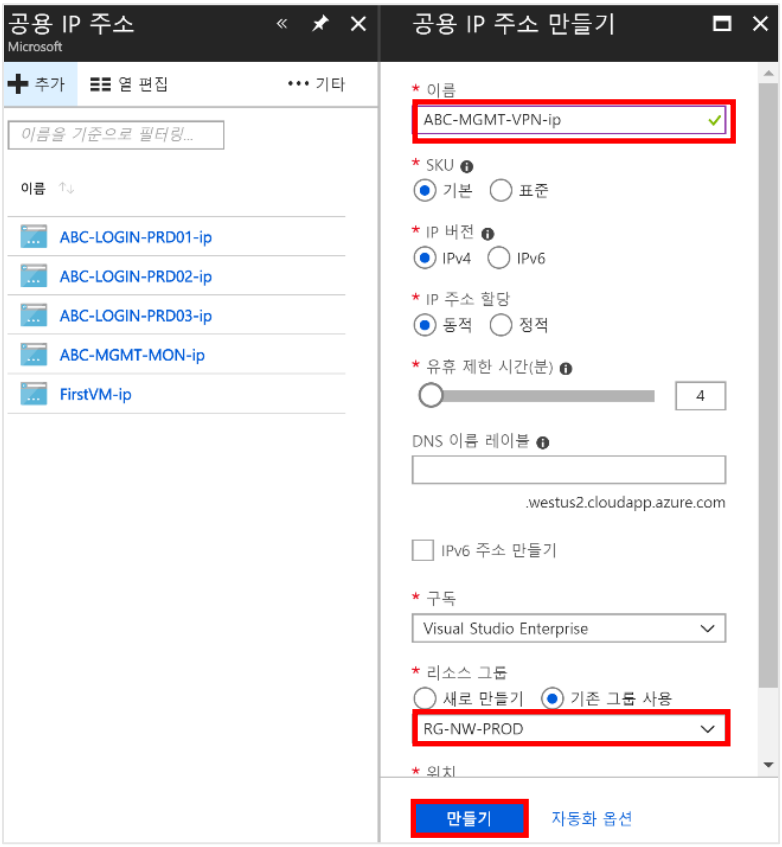
2. 서브넷의 이름에 'GatewaySubnet' 값이 자동으로 채워집니다. Azure 가 서브넷을 게이트웨이 서브넷으로 인식하기 위해 이 값이 필요합니다. 구성 요구 사항에 맞게 게이트웨이 서브넷을 생성합니다. (/27, /28 로 생성하여도 무방합니다.)

3. 아래와 같이 "GatewaySubnet"이 생성된 것을 확인합니다.

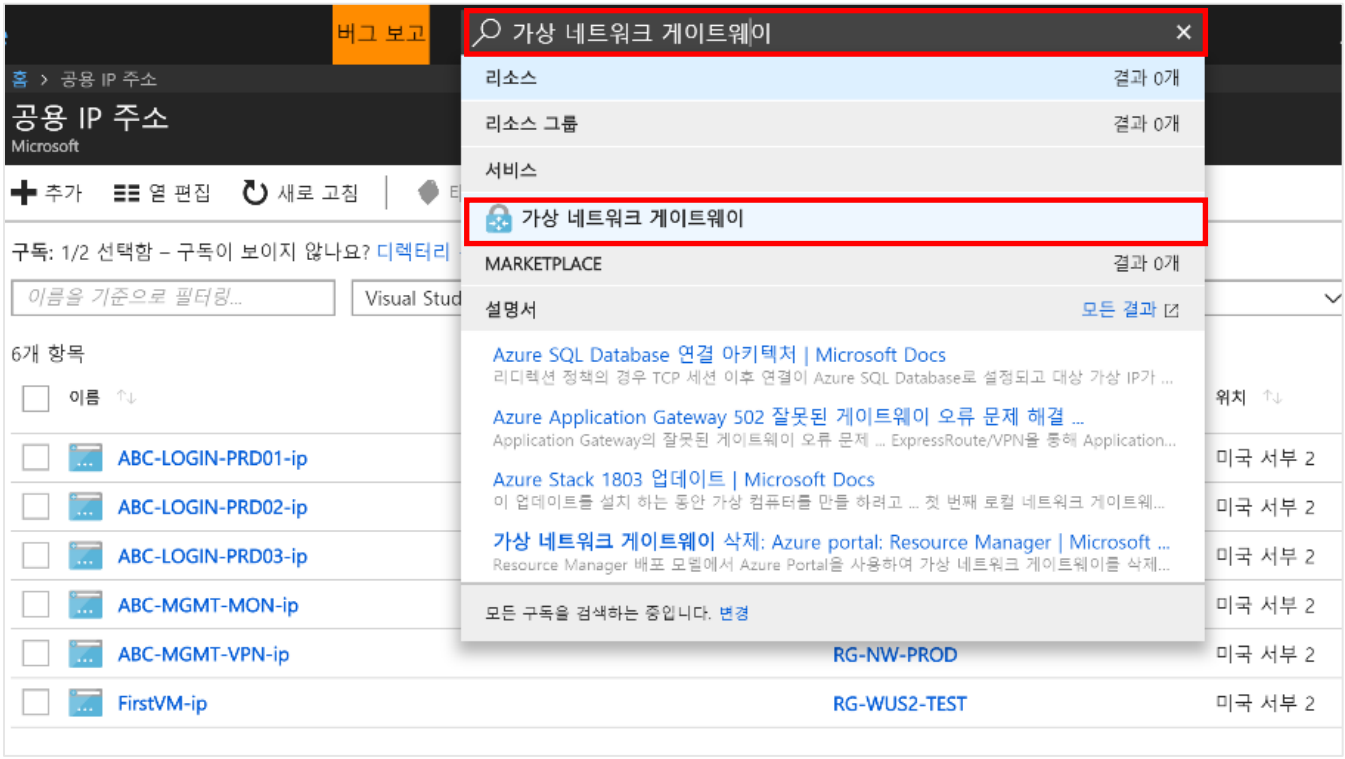


4. 검색 탭에서 "공용 IP 주소"를 검색하여 공용 IP 주소 서비스 페이지로 이동한 뒤, VPN 게이트웨이가 사용할 공용 IP 를 하나 생성하여 줍니다.

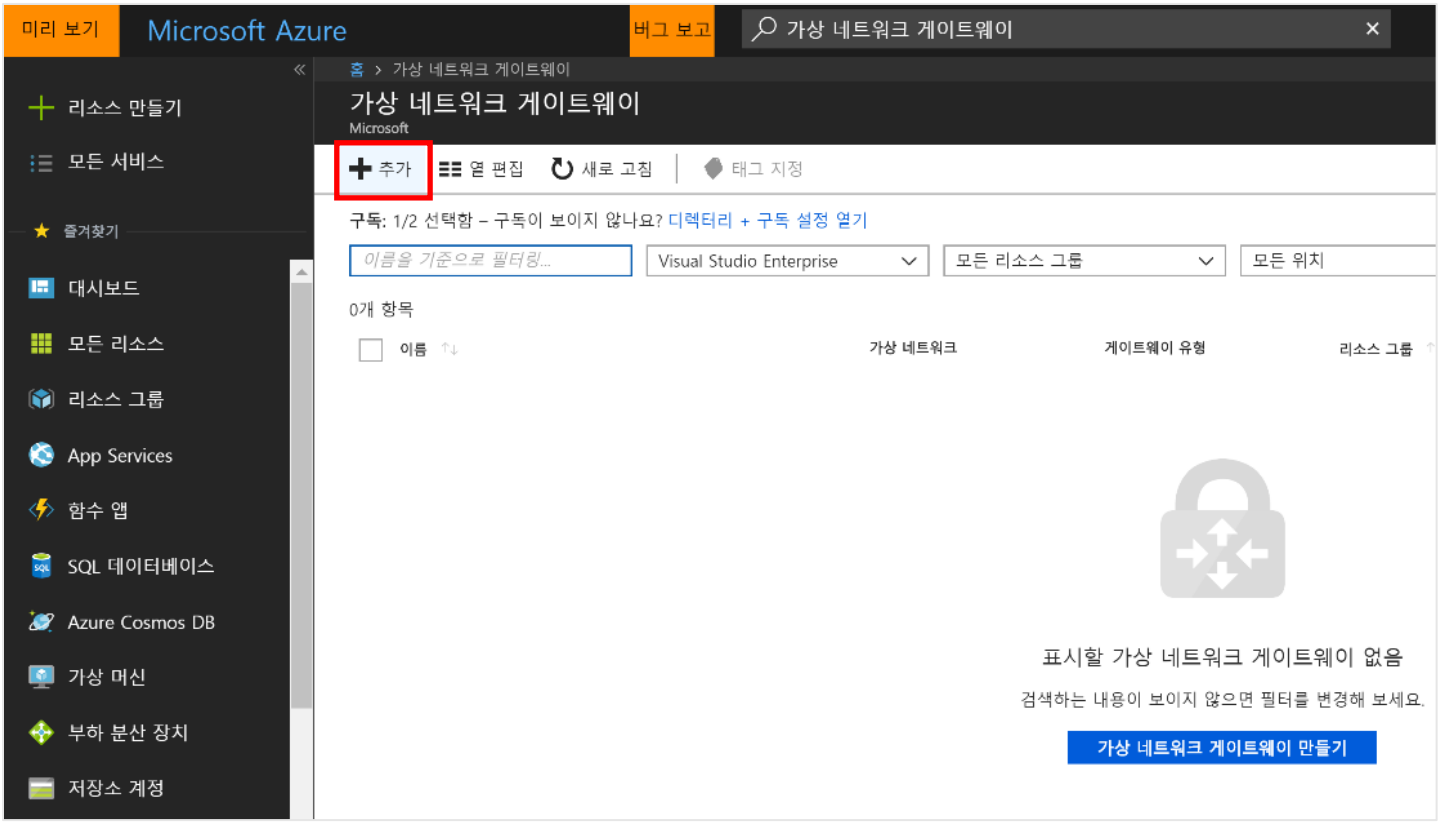
이름 → ABC-MGMT-VPN-ip , 리소스 그룹 → RG-NW-PROD



5. IP 주소를 생성하고 나면, "가상 네트워크 게이트 페이지"로 이동합니다.



6. +추가 버튼을 클릭하여 가상 네트워크 게이트웨이 생성 페이지로 이동합니다.



7. 가상 네트워크 게이트웨이 만들기 페이지에서 가상 네트워크 게이트웨이의 값을 지정합니다.

- **이름 : MGMTGW**
- **게이트웨이 유형 : VPN**
- **VPN 형식 : 경로 기반 VPN**
- **SKU : VPNGw1 (30 개 / 650Mbps)** **참고 URL**
- **위치 : 미국 서부 2 (vNET 의 위치)**
- **가상 네트워크: VNET-ABC-MGMT.**
- **공용 IP 주소 : 기존 항목 사용 – ABC-MGMT-VPN-ip**

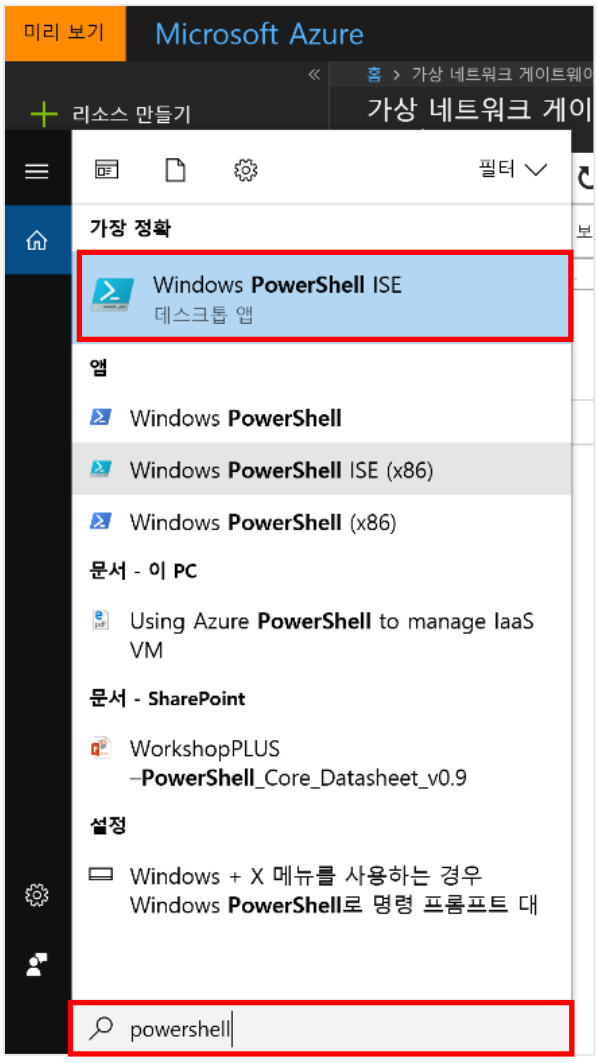
Step 2: 서명된 인증서 생성 (Root / Client) 및 Azure 에 등록

지점 및 사이트 간 VPN 연결을 통해 가상 네트워크에 연결되는 클라이언트를 인증하기 위해 인증서가 사용됩니다. 루트 인증서가 있거나 생성하였으면, Azure 에 공개 키 정보를 업로드합니다. 그러면 루트 인증서는 P2S 를 통한 가상 네트워크 연결을 위해 Azure 에서 '신뢰할 수 있는' 것으로 간주됩니다.

또한 신뢰할 수 있는 루트 인증서에서 클라이언트 인증서를 생성한 후 각 클라이언트 컴퓨터에 인증서를 설치합니다. 클라이언트 인증서는 가상 네트워크에 대한 연결을 시작할 때 해당 클라이언트를 인증하는 데 사용됩니다.

- Windows 10 및 Powershell 을 통한 인증서 생성
- Windows 10 이 아닌 경우 "MakeCert"를 통한 인증서 생성 (하단 URL 가이드를 통하여 생성)
  ➔ https://docs.microsoft.com/ko-kr/azure/vpn-gateway/vpn-gateway-certificates-point-to-site-makecert

1. 현재 사용하고 있는 로컬머신에서 "Windows Powershell ISE"를 실행합니다.



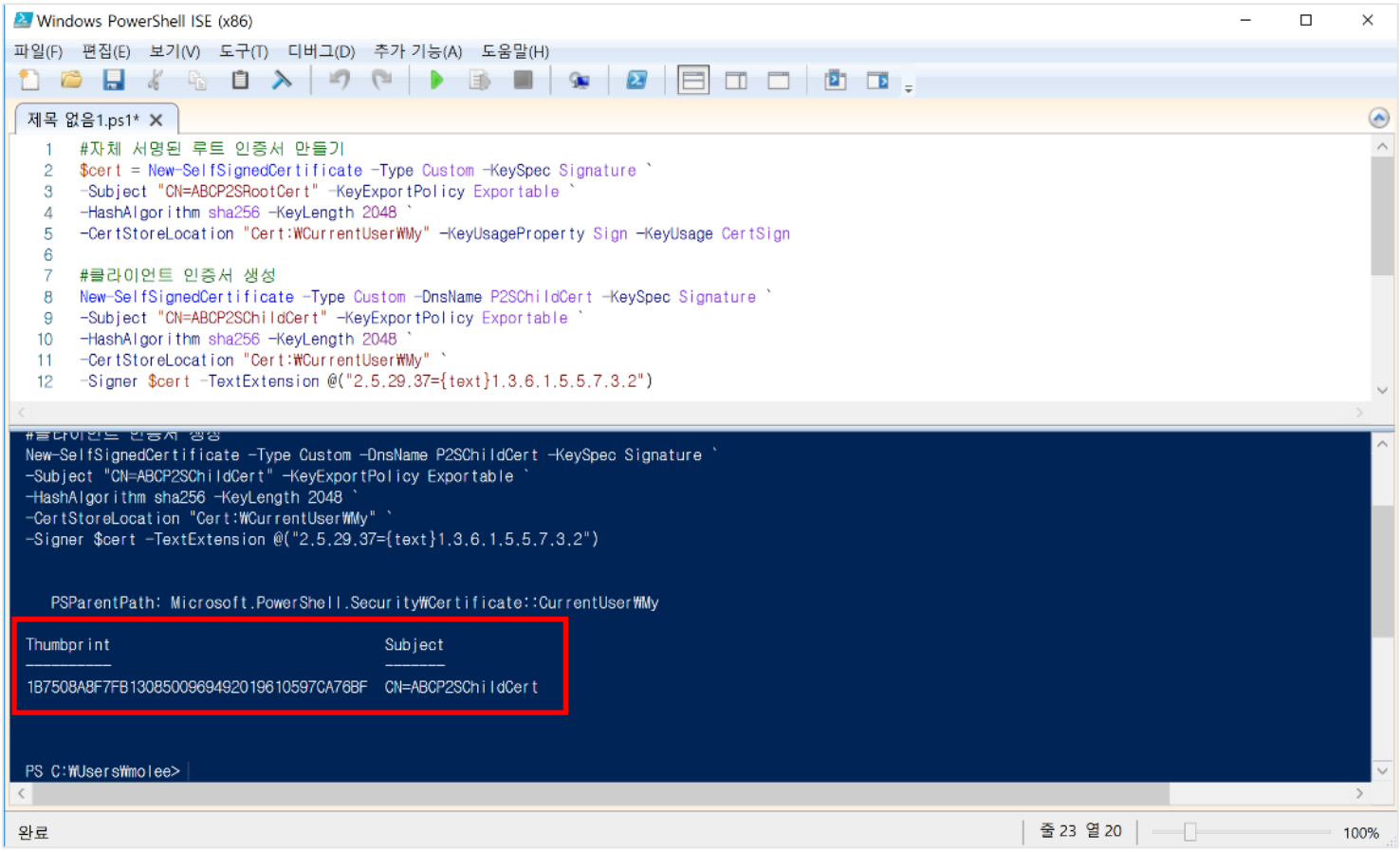
2. 다음 커맨드를 Powershell 에서 실행하여 자체 서명된 루트 인증서를 만듭니다. $cert 변수로 저장되는 커맨드는 자동으로 '**ABCP2SRootCert**'라는 자체 서명된 루트 인증서를 만듭니다.

   다음 커맨드는 $cert 에서 생성된 루트 인증서를 이용하여, '**ABCP2SChildCert**'라는 클라이언트 인증서를 생성합니다. 두 인증서 모두 컴퓨터의 'Certificates - Current User\Personal\Certificates'에 자동으로 설치됩니다.

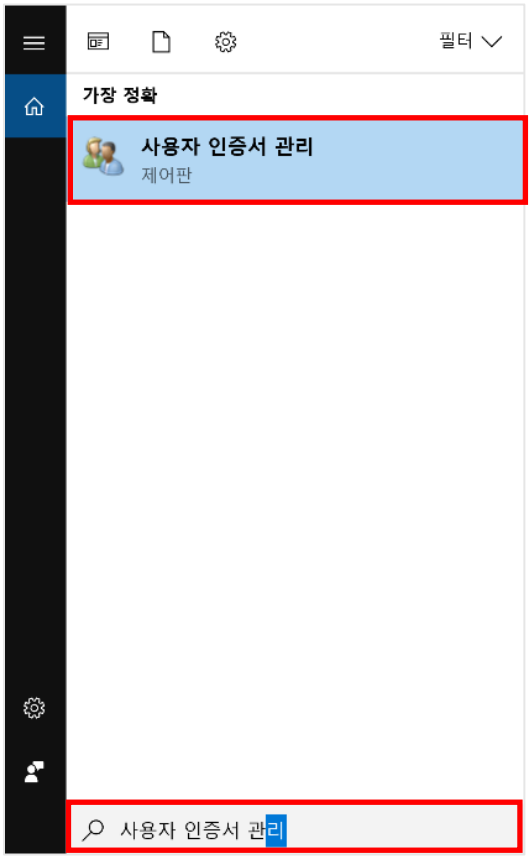
```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=ABCP2SRootCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature -Subject "CN=ABCP2SChildCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

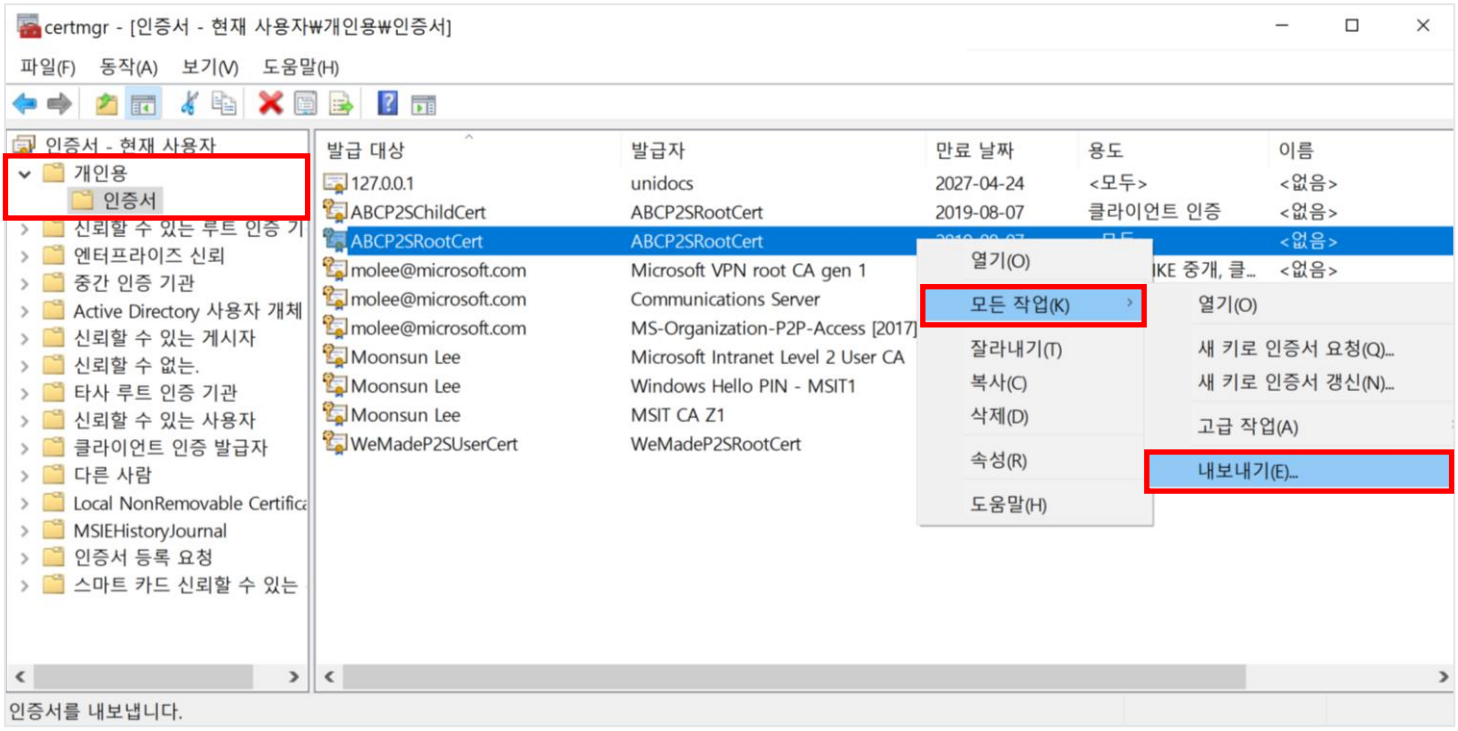
Powershell 에서 위 명령어를 실행하여, 루트/클라이언트 인증서를 각각 생성합니다.



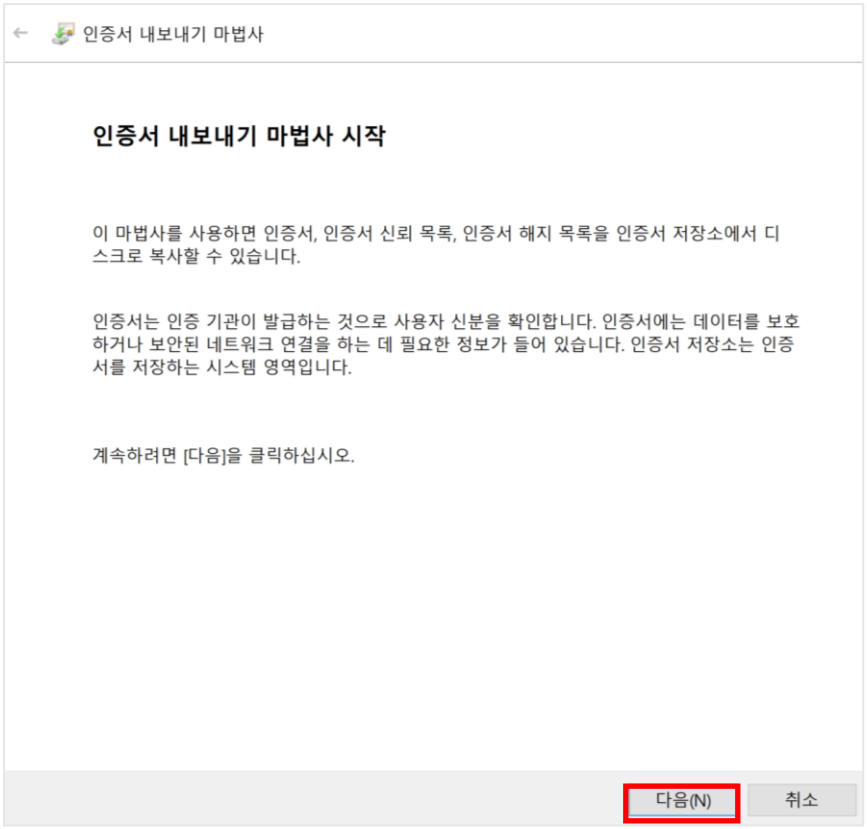
3. 로컬머신에 생성되고 저장된 인증서들을 파일로 추출 하기 위해, Windows 의 "사용자 인증서 관리" 프로그램으로 이동합니다.



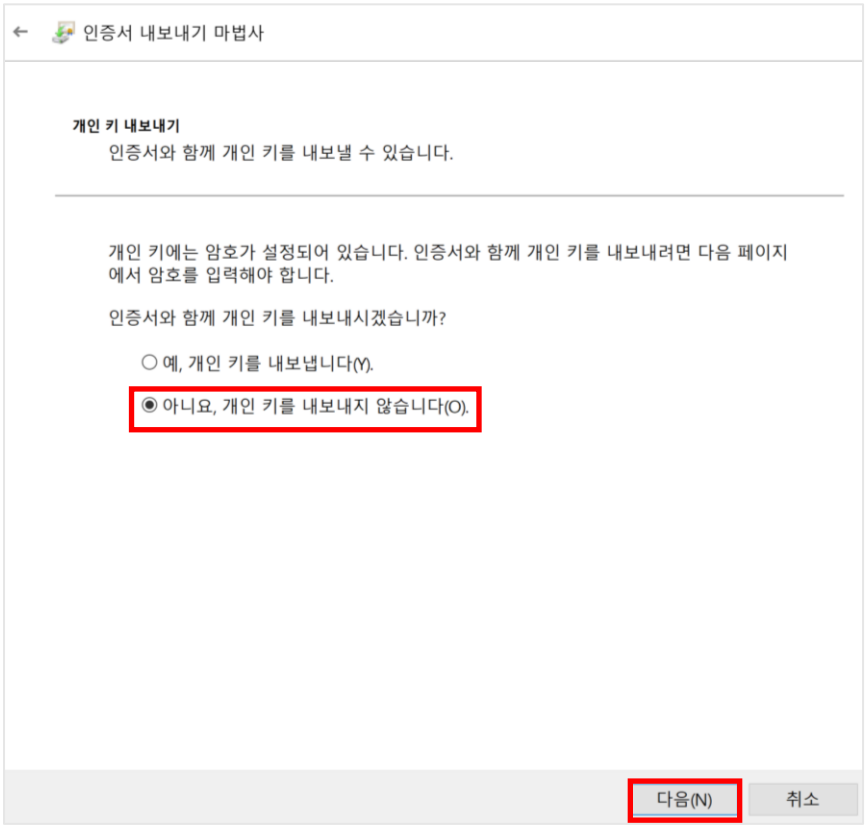
4. "개인용-인증서" 폴더에서 생성된 인증서들을 확인할 수 있습니다. 먼저 루트 인증서인 "ABCP2SRootCert"를 우클릭 하고 "모든 작업-내보내기"를 클릭하여 인증서 내보내기 마법사로 이동합니다.



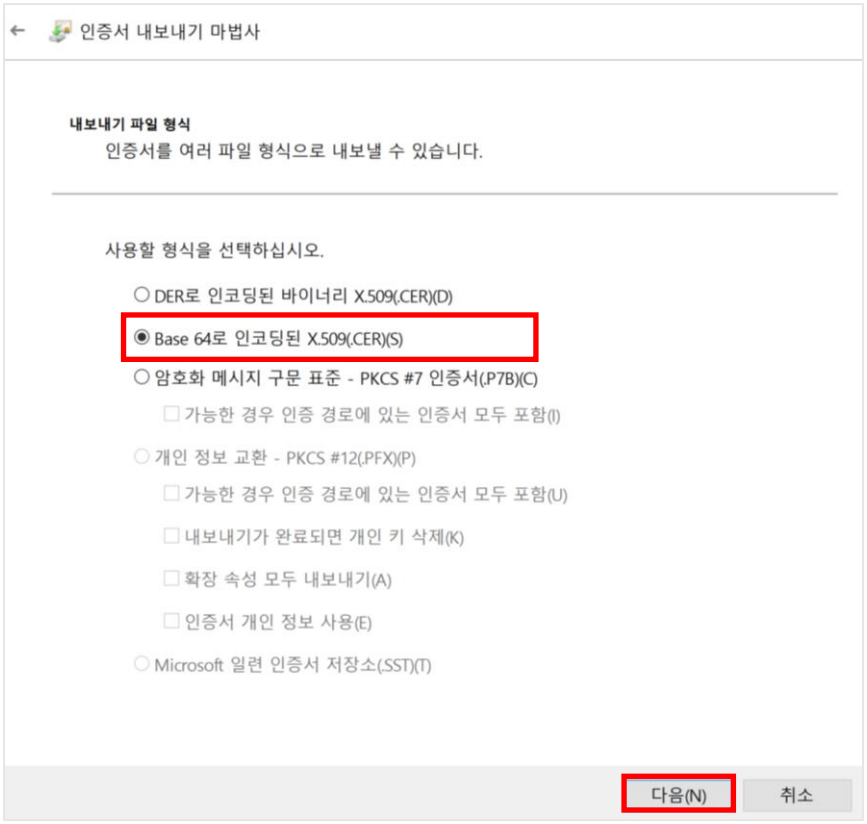
5. 마법사에서 다음을 클릭합니다.



6. 아니요, 개인 키를 내보내지 않습니다. 를 선택한 후 다음을 클릭합니다.

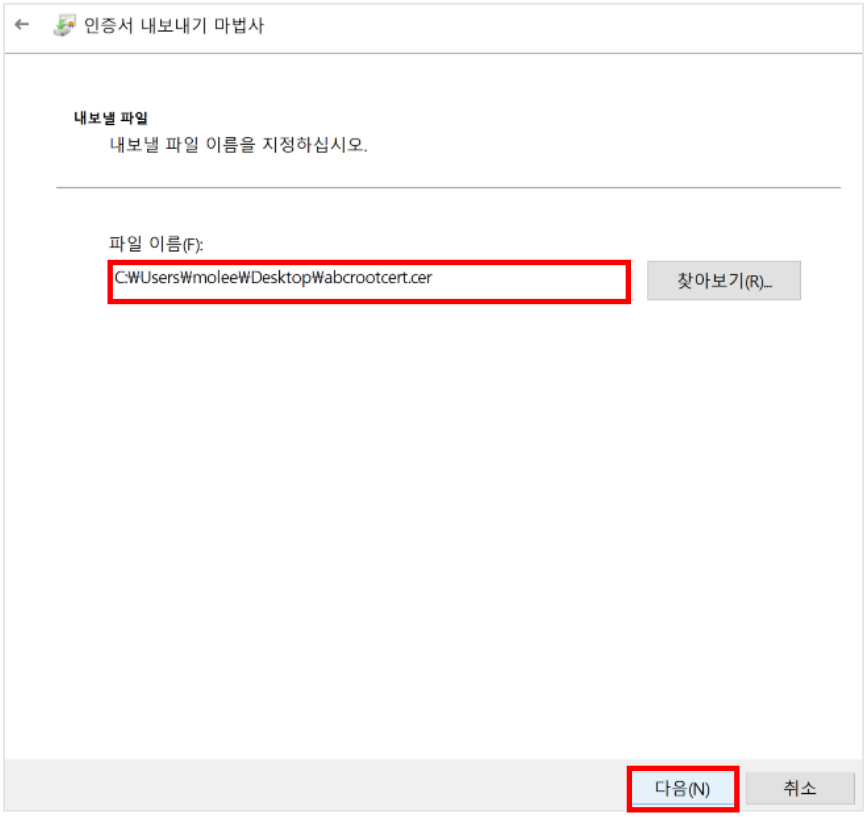


7. 내보내기 파일 형식 페이지에서 **Base 64 로 인코딩된 X.509(.CER)** 를 선택한 후 다음을 클릭합니다.

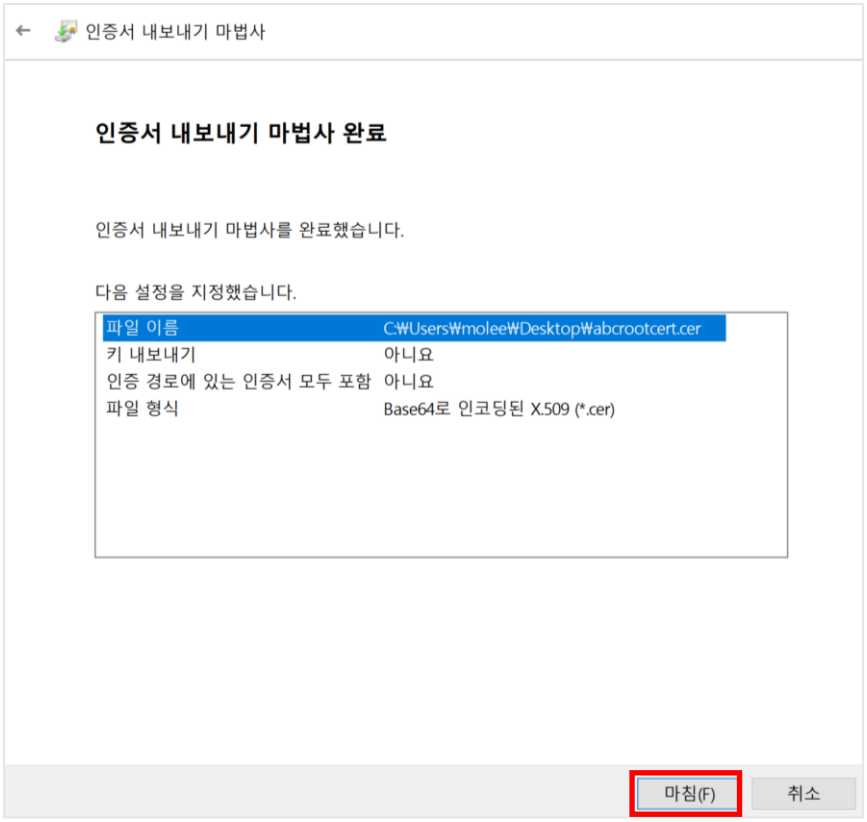


8. 내보낼 파일에서 인증서를 내보내려는 위치와 루트인증서의 파일 이름 입력합니다. 그런 후 다음을 클릭합니다.

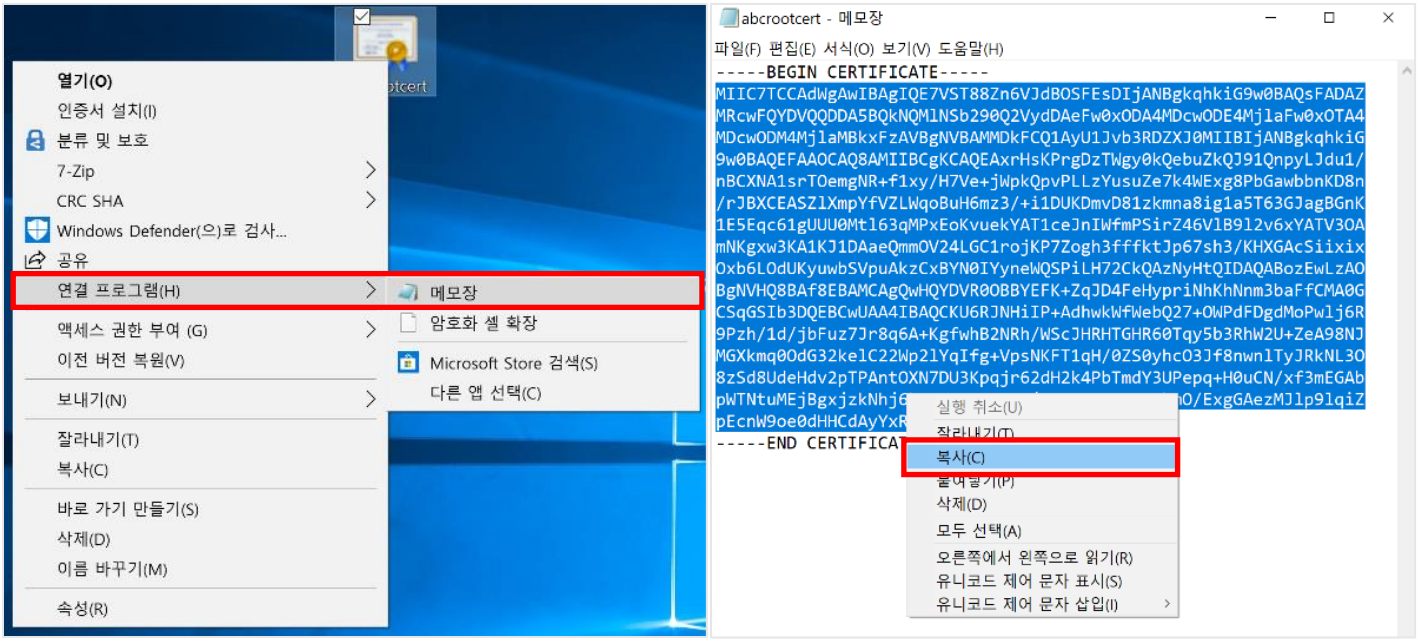
파일명(.cer) → abcrootcert.cer



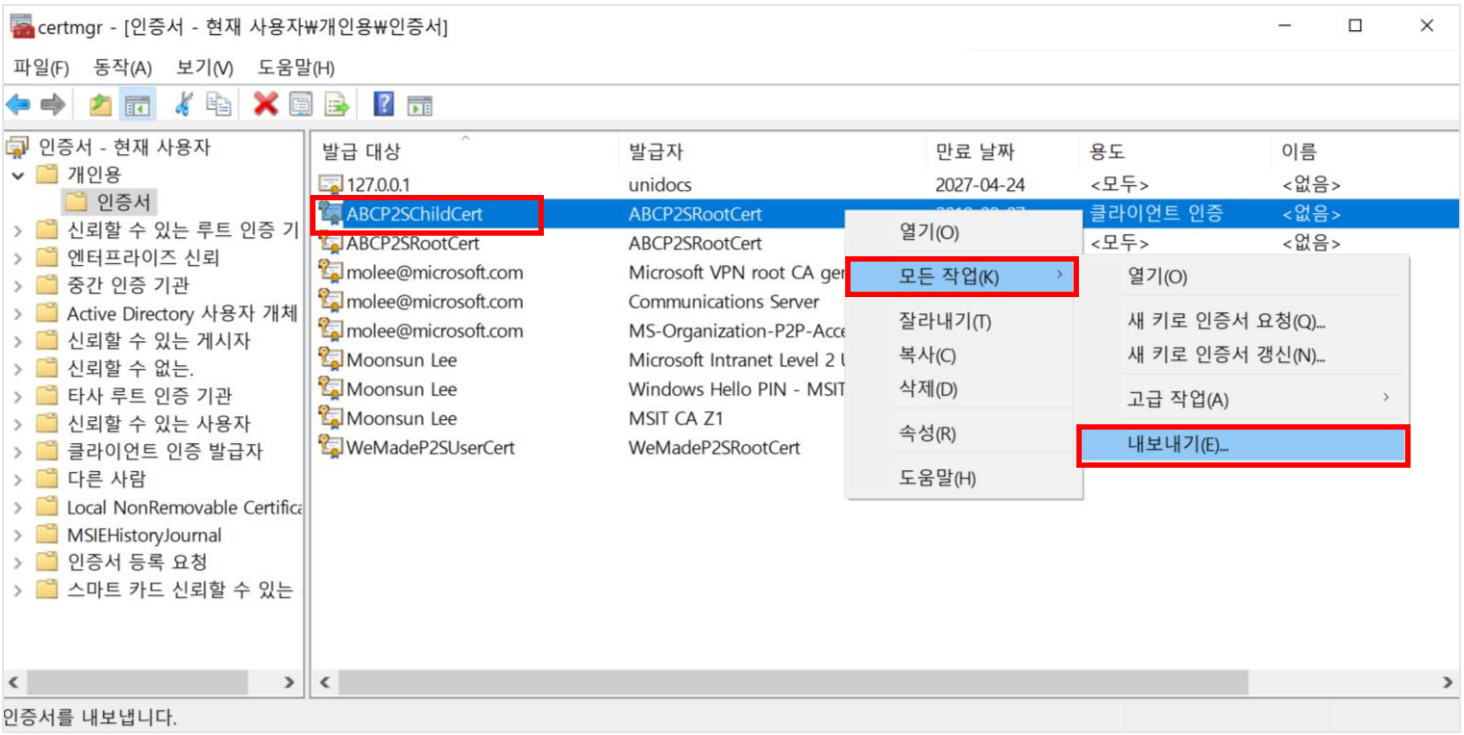
9. 마침을 클릭하여 인증서를 내보냅니다.



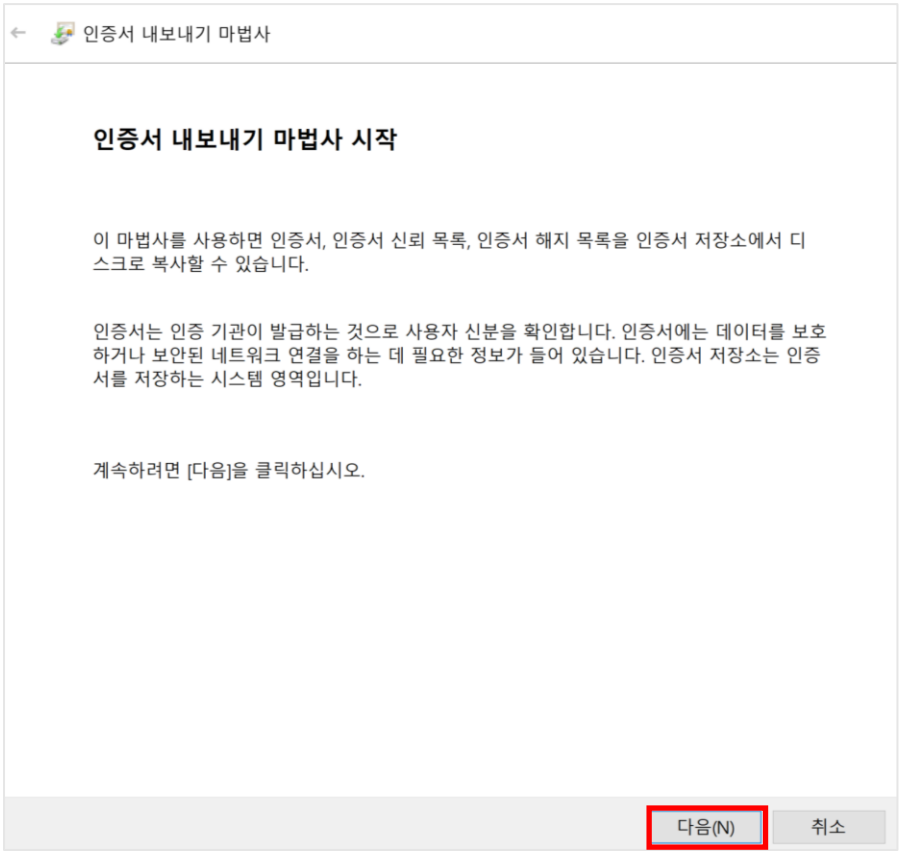
10. 메모장을 사용하여 내보낸 루트 인증서를 열어 키를 복사하여 둡니다. 추후 이 루트 인증서 키를 Azure 에 업로드하여, P2S VPN 인증으로 사용합니다.



11. 이번에는 클라이언트 인증서를 파일로 추출합니다. 내보낼 클라이언트 인증서인 "**ABCP2SChildCert**" 인증서를 마우스 오른쪽 단추로 클릭하고 모든 작업을 클릭한 다음 내보내기를 클릭하여 인증서 내보내기 마법사를 엽니다.

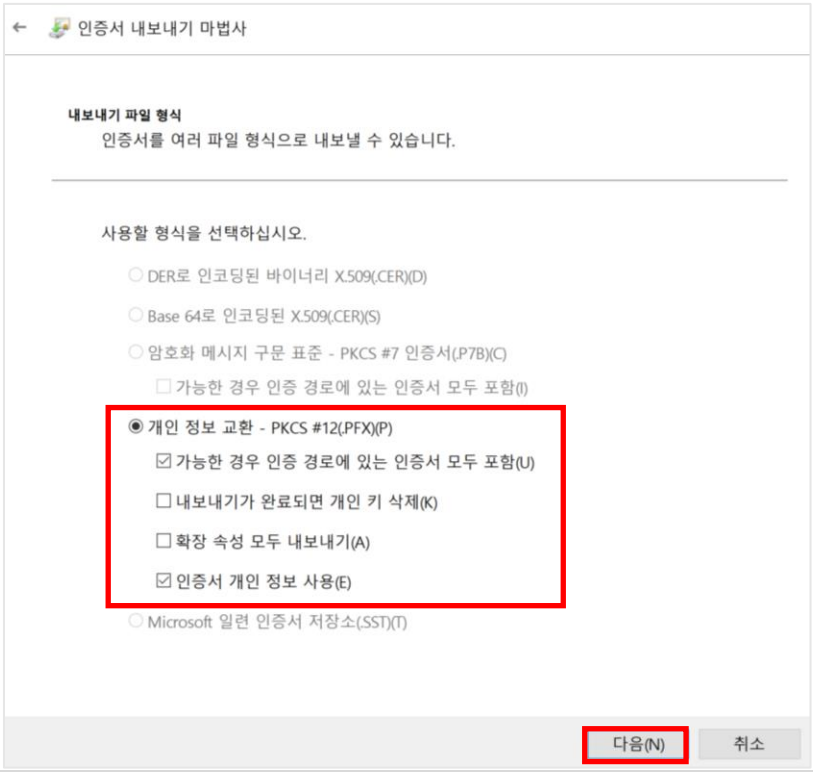


12. 인증서 내보내기 마법사에서 다음을 클릭하여 계속합니다.

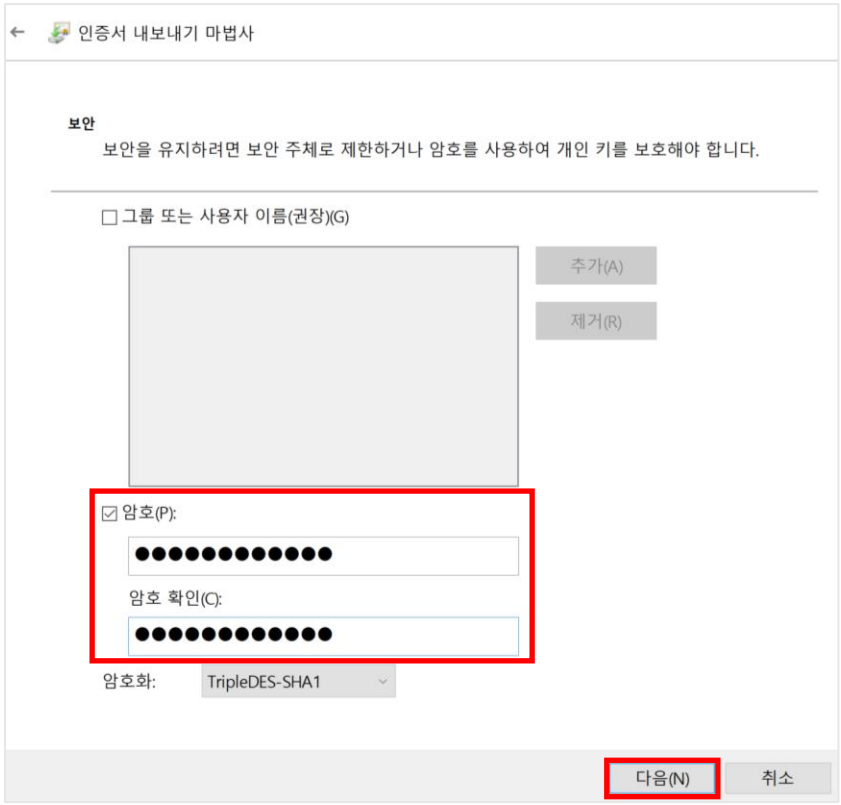


13. "예, 개인 키를 내보냅니다."를 선택하고 다음을 클릭합니다.

14. 파일 내보내기 형식 페이지에서 선택된 기본값을 유지합니다. "가능한 인증 경로에 있는 인증서 모두 포함"을 선택했는지 확인합니다. 이 설정은 성공적인 클라이언트 인증에 필요한 루트 인증서 정보를 추가로 내보냅니다. 이를 사용하지 않으면 클라이언트에 신뢰할 수 있는 루트 인증서가 없어 클라이언트 인증에 실패합니다. 그런 후 다음을 클릭합니다.



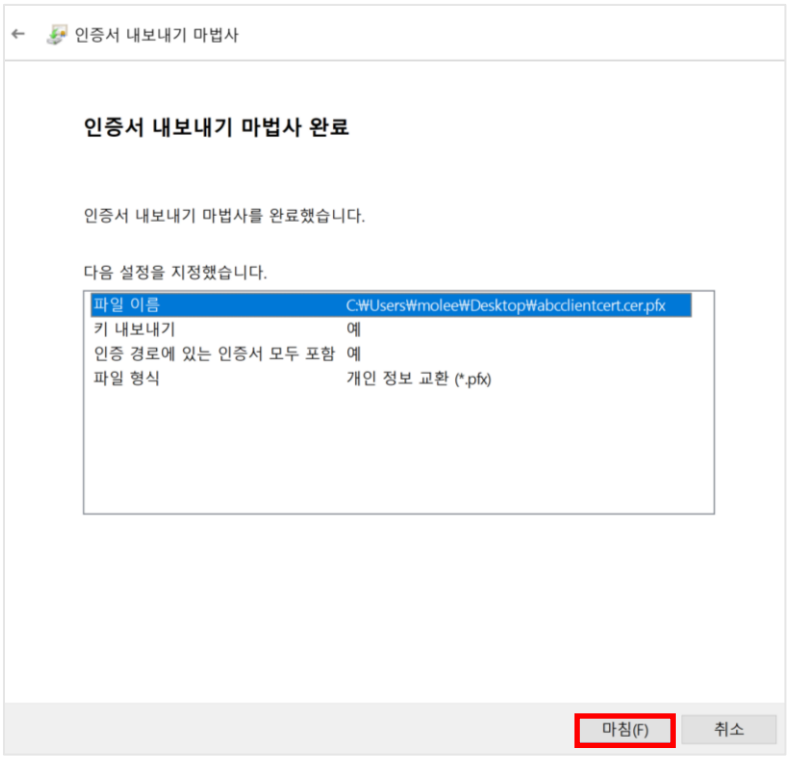
15. 보안 페이지에서 암호를 입력하여 개인 키를 보호합니다. 암호를 입력한 뒤, 다음을 클릭합니다.



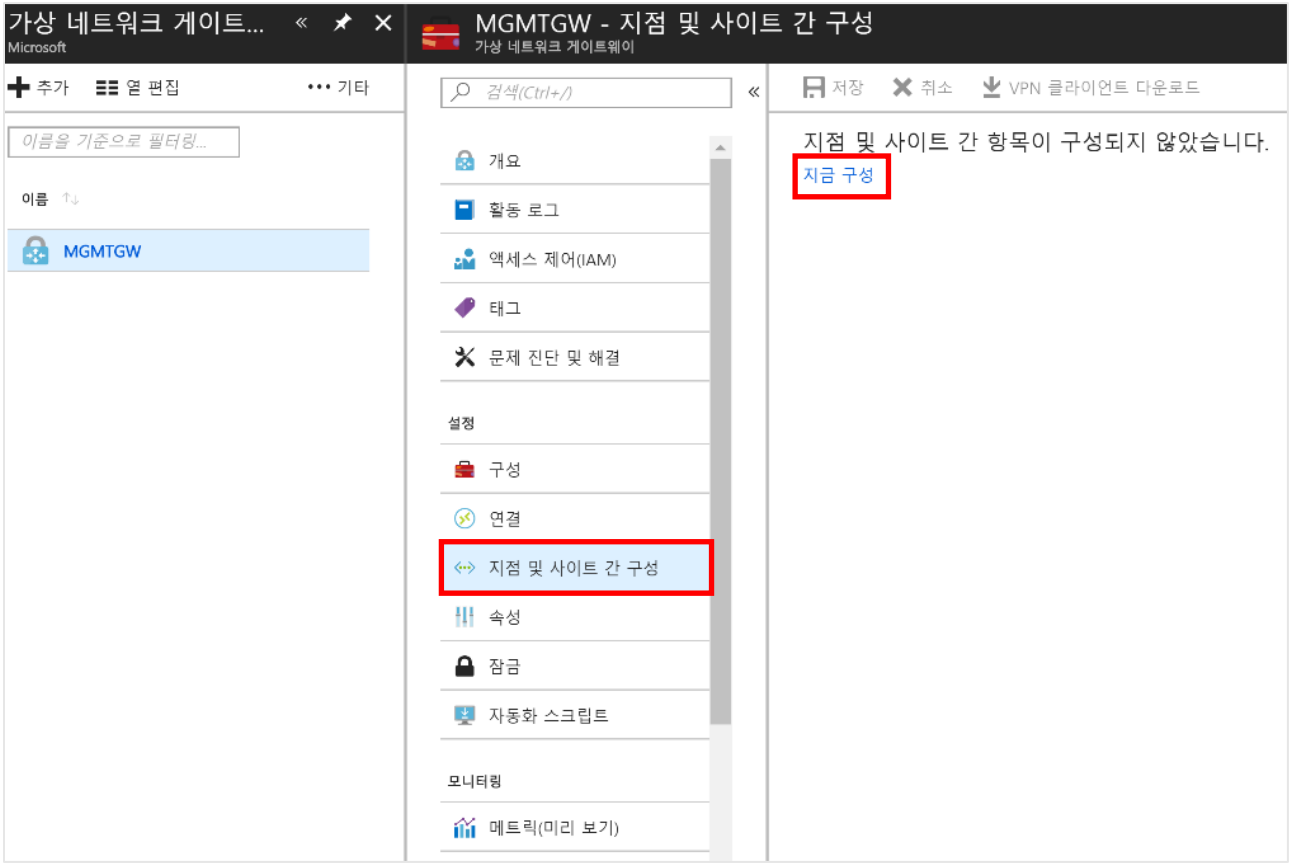
16. 내보낼 파일에서 인증서를 내보내려는 위치와 클라이언트 인증서의 파일 이름 입력합니다. 그런 후 다음을 클릭합니다.

파일명(.pfx) → abcclientcert.pfx

17. 마침을 클릭하여 인증서를 내보냅니다. 이 클라이언트 인증서를 이용하여, P2S 연결을 통하여 가상 네트워크에 연결할 수 있습니다. 다른 머신에서 접속하려는 경우, 방금 추출한 클라이언트 인증서를 로컬로 설치해야 합니다.



18. 포탈로 돌아와, "가상 네트워크 게이트웨이-지점 및 사이트간 구성" 메뉴로 이동하여 "지금 구성" 버튼을 클릭합니다.

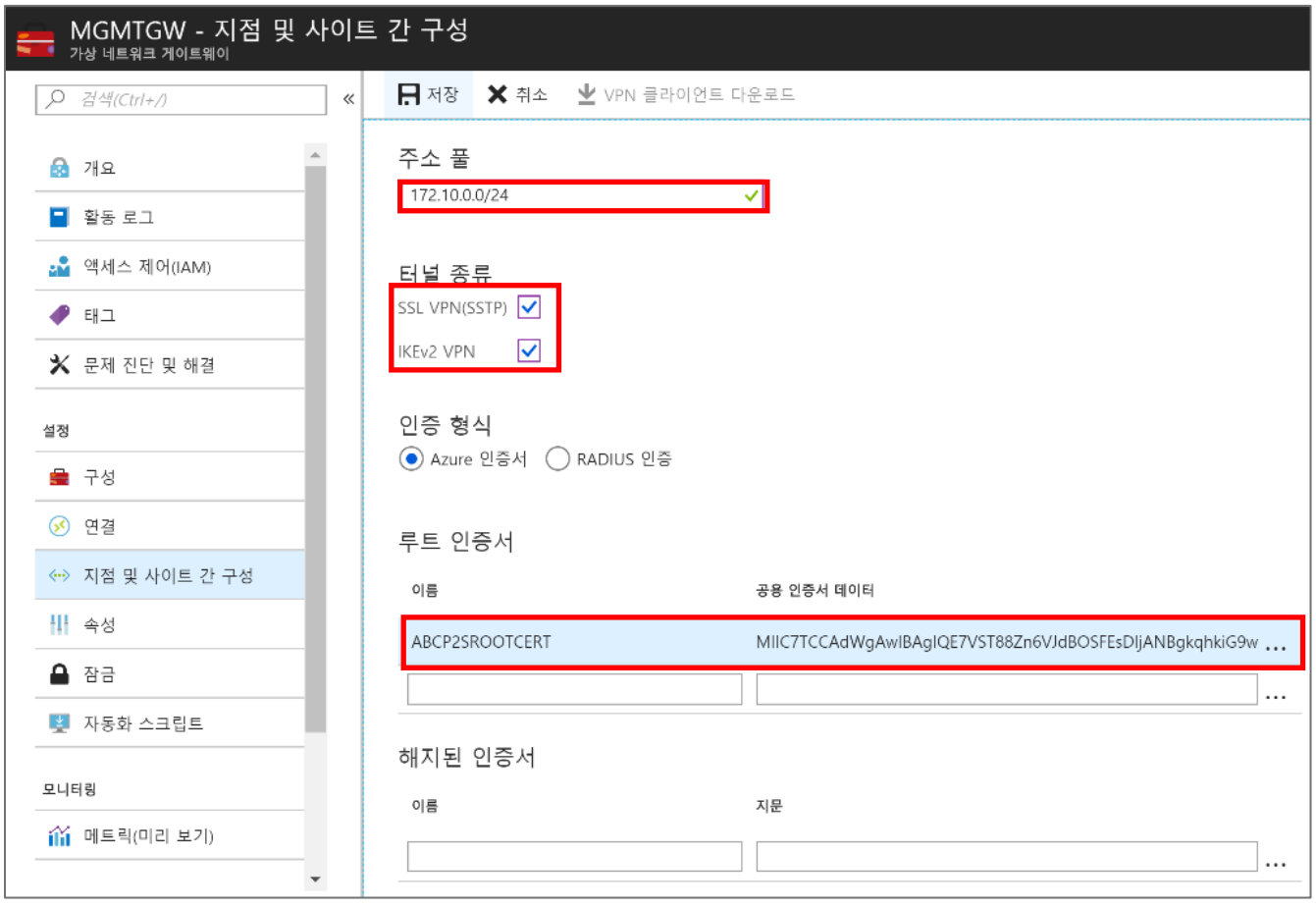


19. 지점 및 사이트 간 구성 페이지의 주소 풀 상자에서 사용하려는 개인 IP 주소 범위를 추가합니다. VPN 클라이언트는 동적으로 지정된 범위에서 IP 주소를 수신합니다. 클라이언트 주소 풀은 사용자가 지정한 개인 IP 주소 범위입니다. 연결 원본이 되는 온-프레미스 위치 또는 연결 대상이 되는 가상 네트워크와 겹치지 않는 개인 IP 주소 범위를 사용합니다.

    터널 종류를 선택할 수 있습니다. 두 개의 터널 옵션은 SSTP 및 IKEv2 입니다. Windows 클라이언트는 IKEv2 를 먼저 시도하고 연결되지 않는 경우 SSTP 로 대체합니다. 그 중 하나 또는 둘 다를 사용하도록 선택할 수 있습니다.
    인증 형식을 Azure 인증서로 선택합니다.

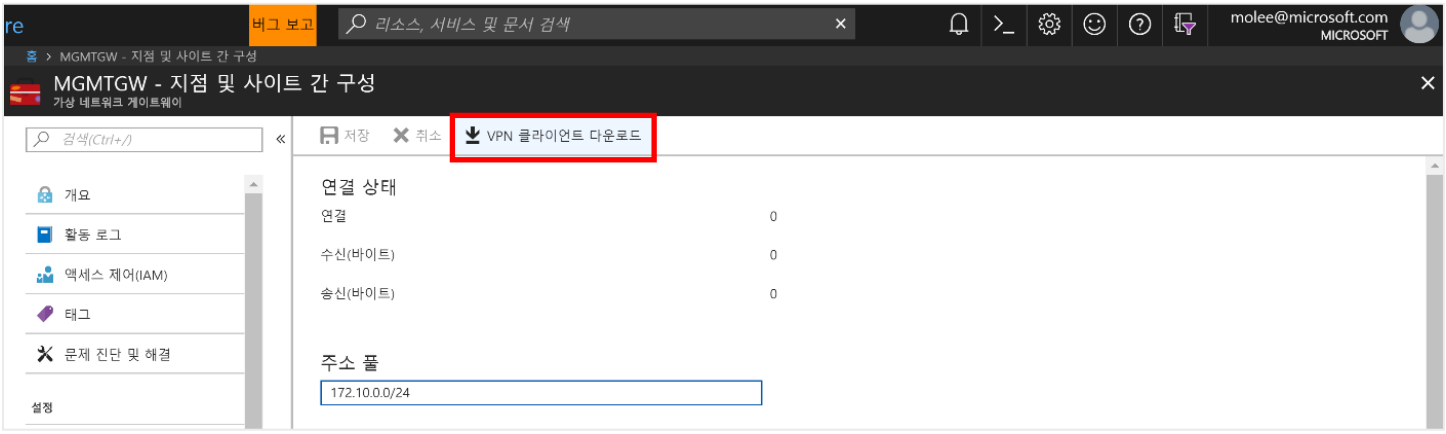
    루트 인증서는 최대 20 개까지 추가로 업로드할 수 있습니다. 공용 인증서 데이터가 업로드 되면 Azure 는 이 데이터를 사용하여 신뢰할 수 있는 루트 인증서에서 생성된 클라이언트 인증서를 설치한 클라이언트를 인증합니다. 10 번 단계에서 복사한 루트 인증서의 공개 키 정보를 Azure 에 업로드합니다. 복사한 공개 키를 공용 인증서 데이터 필드에 붙여 넣습니다. 인증서의 이름을 지정한 다음 저장을 클릭합니다.

    - 주소 풀 → 172.10.0.0/24
    - 터널 종류 → SSL VPN(SSTP) and IKEv2 VPN
    - 인증 형식 → Azure 인증서
    - 루트 인증서 → 이름 : ABCP2SRootCert, 공용 인증서 데이터 : 복사한 루트 인증서 공용 키

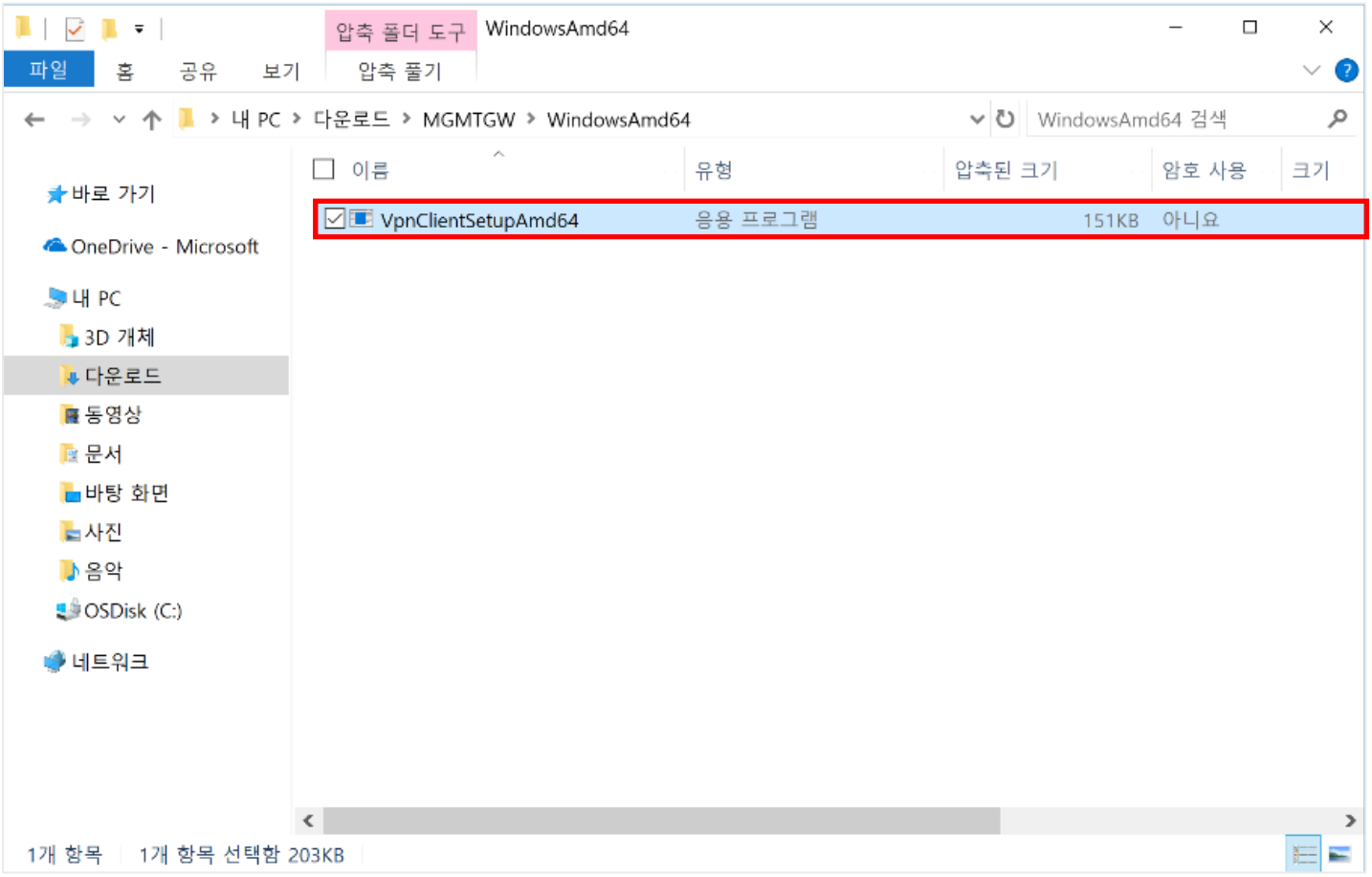


Step 3: 로컬머신에 Azure VPN 클라이언트 설치

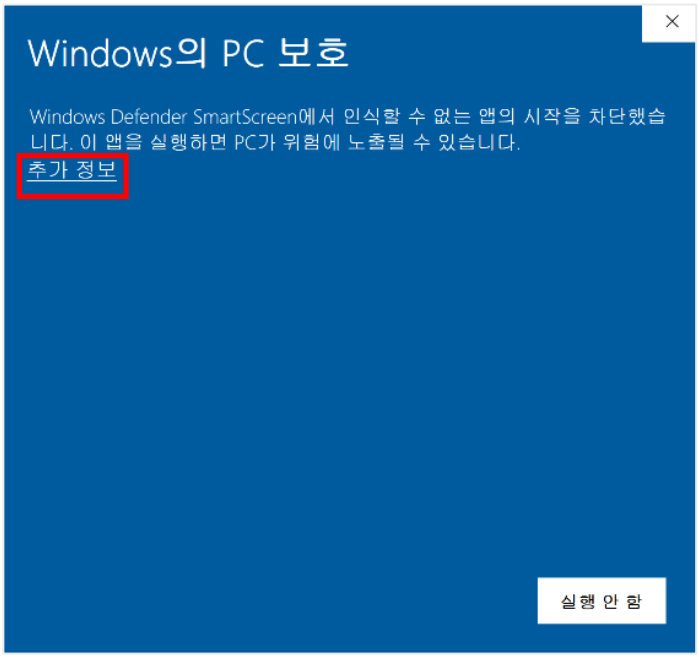
1. 구성이 완료되면, "VPN 클라이언트 다운로드" 버튼을 클릭하여, Azure VPN 클라이언트 압축파일을 다운받습니다.

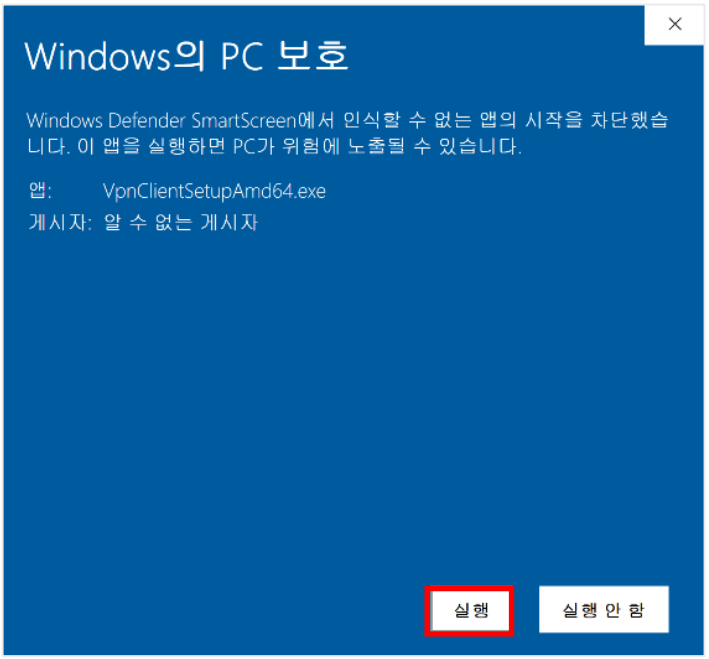


2. 포탈에서 다운로드 된 압축파일을 다운받아, "WindowsAMD64 폴더 내 VPNClientSetupAMD64.exe"파일을 실행시켜 Azure VPN 클라이언트를 VPN 접속을 이용하려는 로컬머신에 설치합니다.



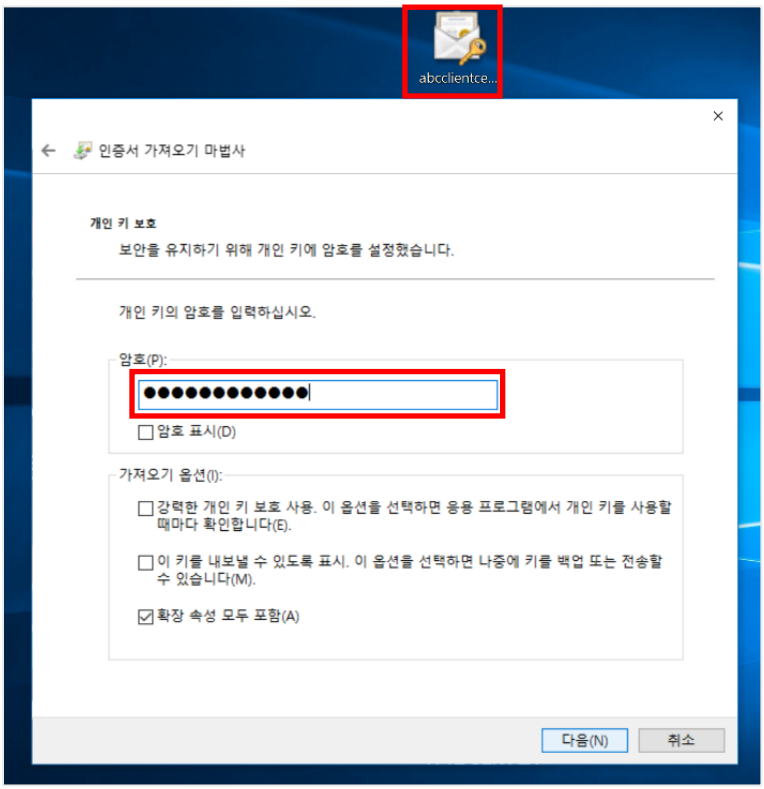
3. "추가 정보" 버튼을 클릭하고, "실행" 버튼을 클릭하여 차단된 파일을 허용하고 다운로드 받은 클라이언트 설치 파일을 실행할 수 있도록 합니다.





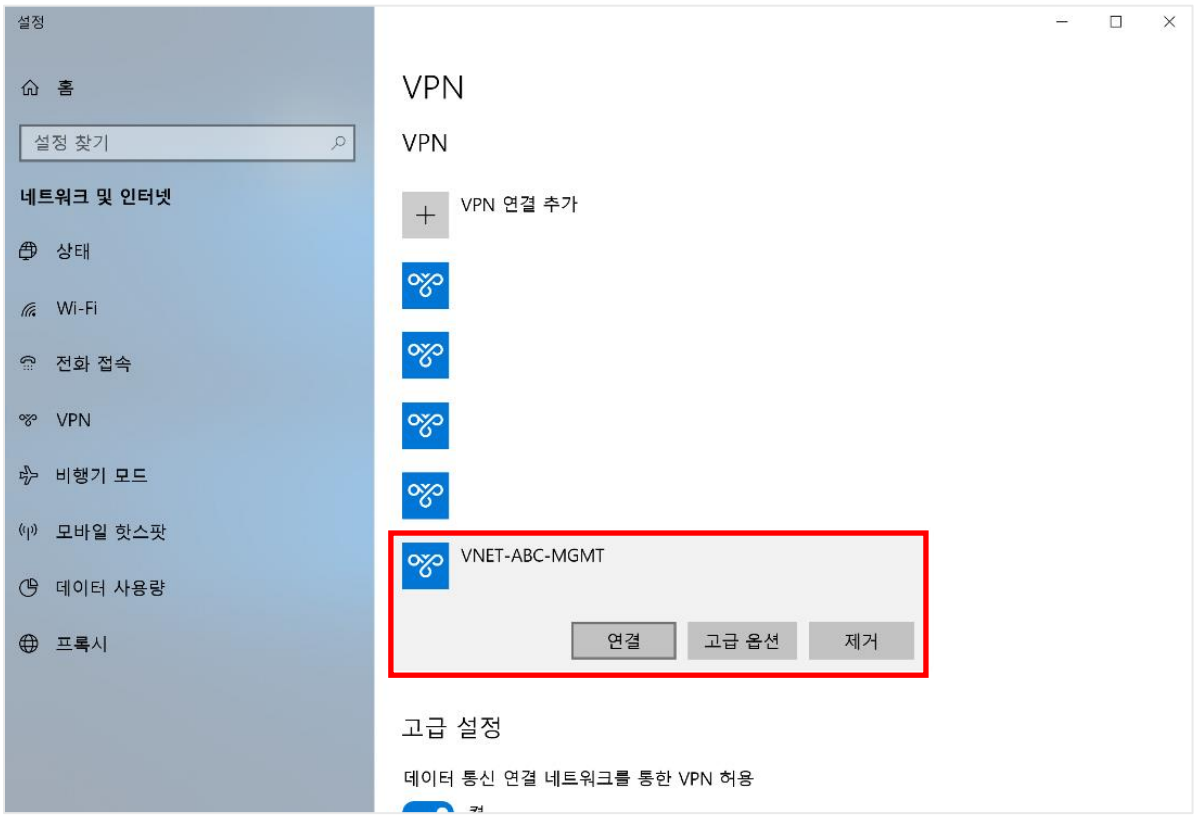
cf. 실습을 실행한 PC 에는 이미 클라이언트 인증서가 존재하지만, 그 외의 클라이언트 컴퓨터에서 P2S 연결을 만들려는 경우 클라이언트 인증서를 설치해야 합니다. 클라이언트 인증서를 설치하는 경우 실습에서 클라이언트 인증서를 내보낼 때 만든 암호가 필요합니다.

→ Azure VPN 클라이언트와 인증서를 VPN 을 이용하려는 컴퓨터에서 실행 및 설치하여 VPN 을 이용할 수 있습니다.

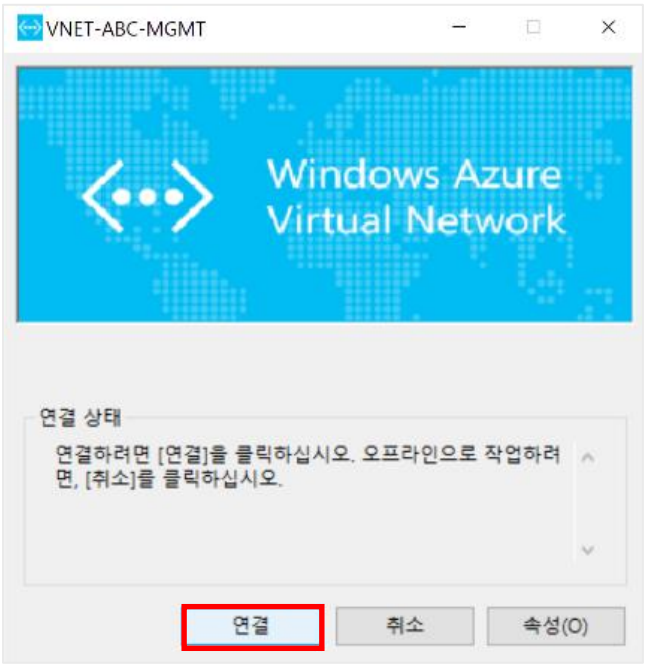


4. VPN 클라이언트 설치가 완료되면, 무선인터넷에 "VNET-ABC-MGMT"의 VPN 세팅이 완료된 것을 확인 할 수 있습니다. "VNET-ABC-MGMT" 버튼을 클릭하여 VPN 설정으로 이동합니다.

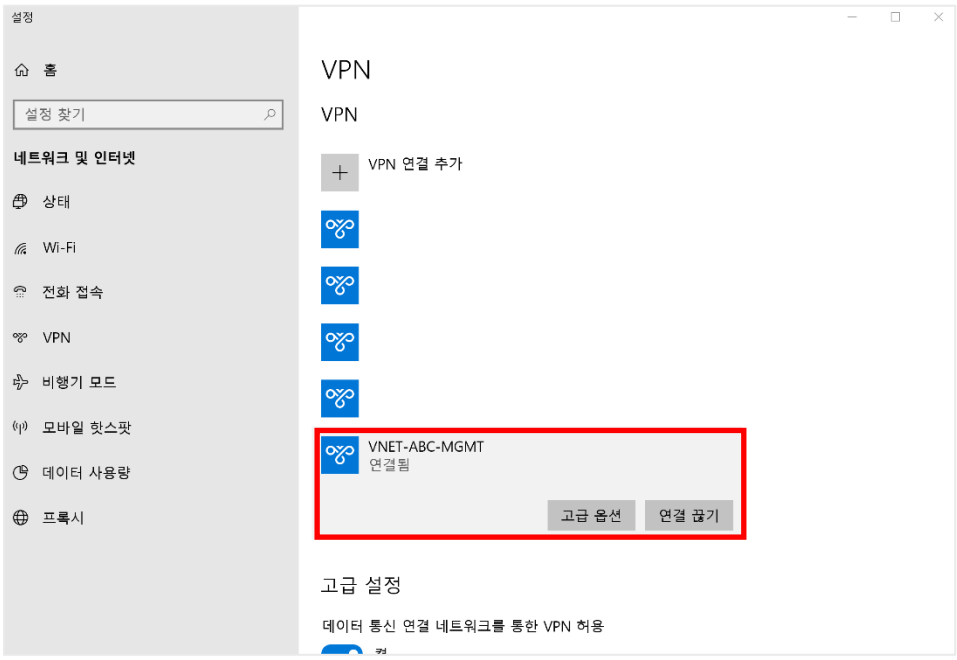
5. "연결" 버튼을 클릭하여 Azure VPN 클라이언트를 실행합니다.



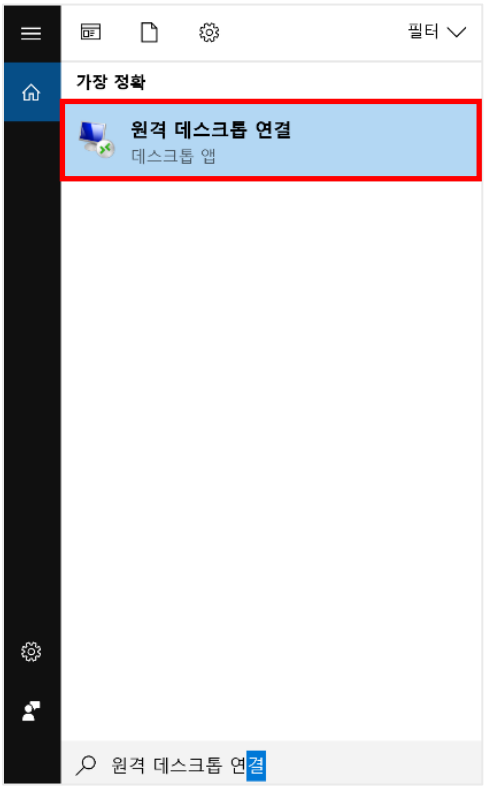
6. Azure VPN 클라이언트가 실행되면 "연결" 버튼을 클릭하여 "VNET-ABC-MGMT"로 VPN 연결을 시도합니다. 설정에 따라 클라이언트 인증서의 암호를 입력해야 할 수도 있습니다.



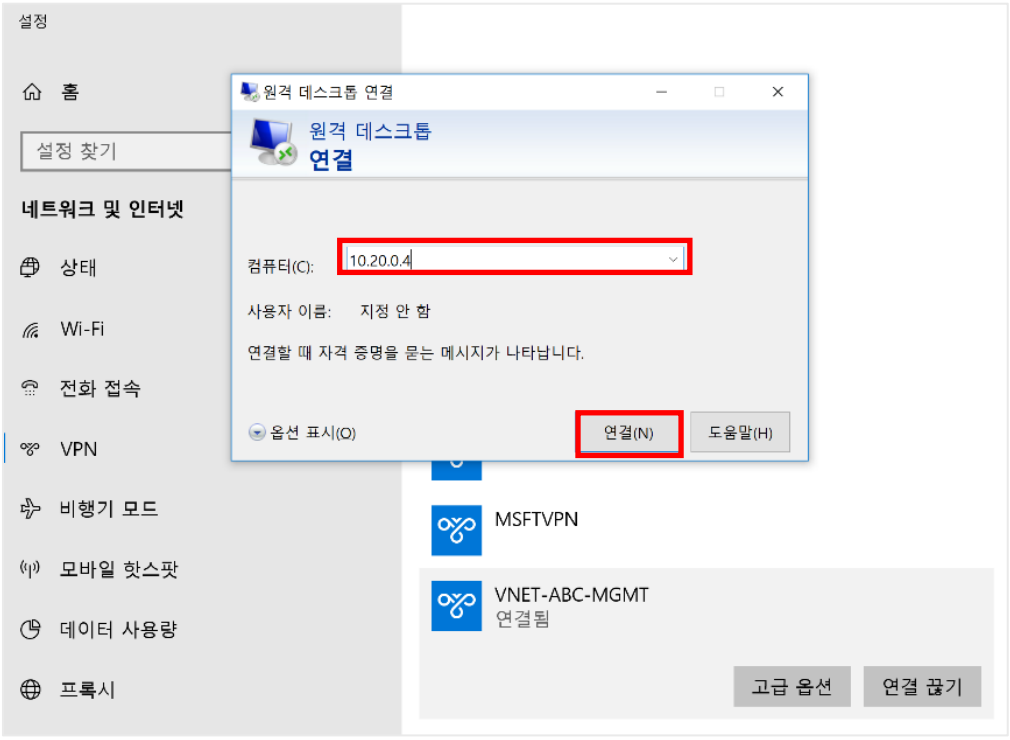
7. 아래와 같이 VPN 연결이 완료되었습니다. 이제 Azure 가상 네트워크의 사설 IP 를 통하여 해당 로컬머신과 통신이 잘 되는지 검증해보겠습니다.



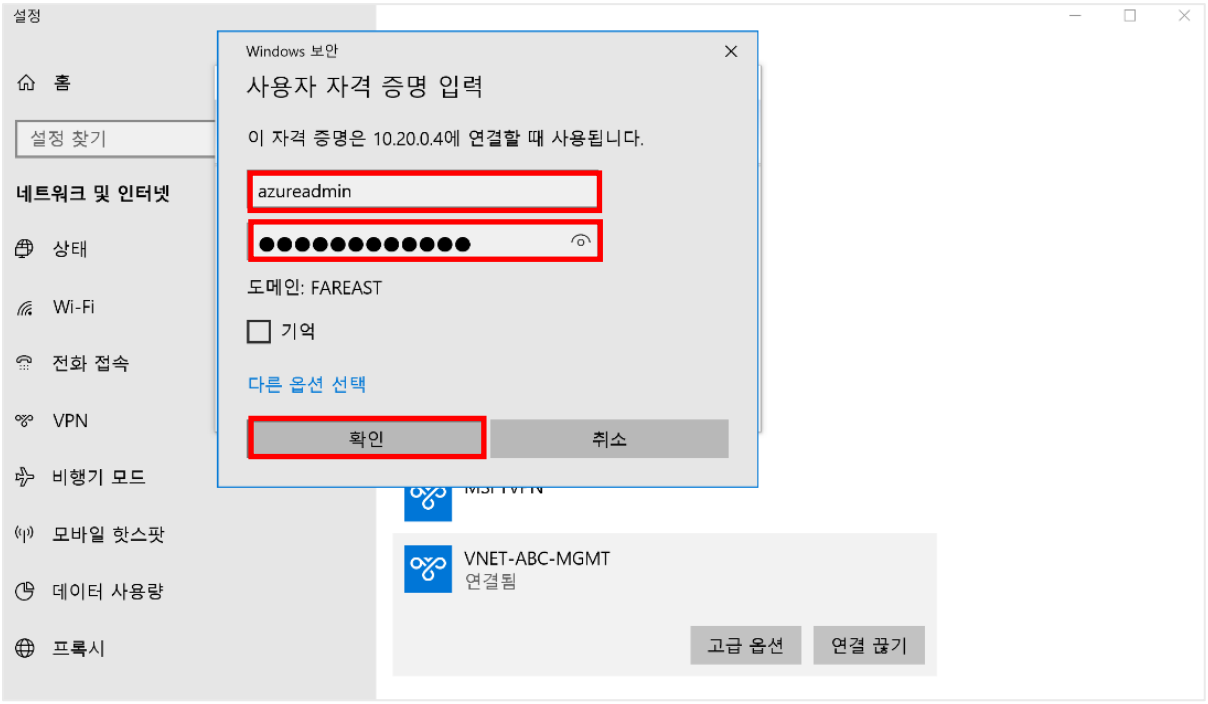
8. 로컬머신에서 "원격 데스크톱 연결" 앱을 실행시켜, "VNET-ABC-MGMT"에 생성되어 있는 "ABC-MGMT-MON"의 사설 IP 로 RDP 접속을 시도합니다.



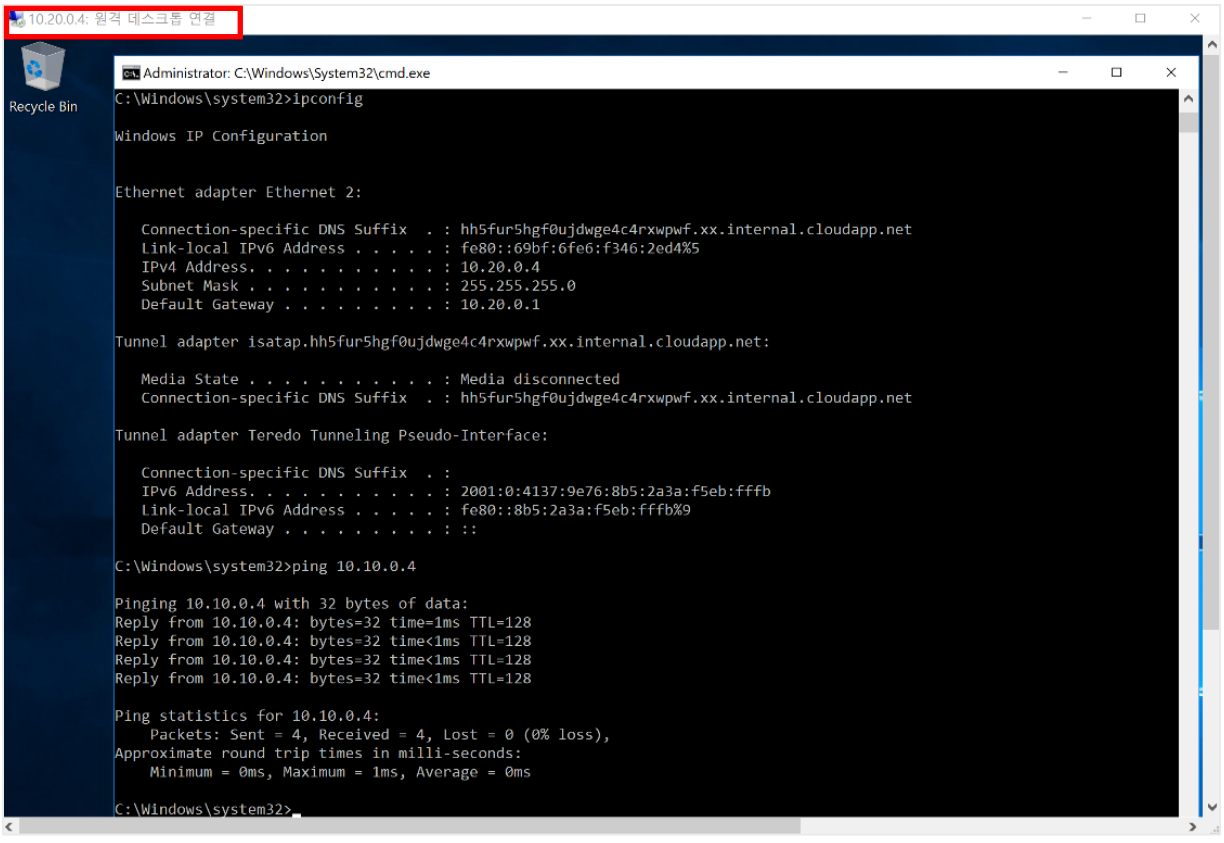
9. "ABC-MGMT-MON"의 사설 IP 정보를 확인하고, IP 정보를 입력한뒤 "연결" 버튼을 클릭합니다.



10. 해당 가상머신의 계정정보를 입력합니다.



11. RDP 접속이 성공적으로 완료되고, VPN 성공적으로 연결된 것을 확인할 수 있습니다.



12. 실습이 완료되면 RDP 연결을 종료하고, VPN 연결을 종료합니다.