Microsoft Azure

VNet-to-vnet(고급)

Hyun Suk Shin (AZURE CSA)

2016

VNet-to-VNet 구성하기 (고급)

본 실습을 통해 Azure Portal에서 서로 다른 두 리전(Region)에 Virtual Network를 각각 만들고 두 Virtual Network 간 VPN으로 연결하여 통신 환경을 구성합니다.

1. 실습을 위해서 사전에 계정과 구독 그리고 실습을 위한 관련 도구(tool)을 다운로드 받습니다.
   1. Azure 계정과 구독
      1. Azure에 접속하기 위해서는 Microsoft 계정이 필요합니다. Microsoft 계정이 없는 경우 <http://msn.com>에서 새로 생성할 수 있습니다.
         1. <http://msn.com> 을 방문하여 오른쪽 상단에 ‘로그인’을 클릭하고 ‘계정을 만드세요’를 클릭합니다.

|  |  |
| --- | --- |
|  |  |

* + - 1. 계정을 생성 할 때 아래와 이미 존재하는 회사 메일 주소를 사용할 수 있습니다.

|  |
| --- |
|  |

* + 1. 제공된 Azure Free Pass를 사용하여 무료 구독을 생성합니다. Free Pass는 30일 동안 제공된 금액 미만으로 사용이 가능하며 제공된 비용을 초과하게되는 경우 또는 30일이 경과하는 경우는 자동으로 중지 됩니다.
  1. 리눅스 가상 컴퓨터에 접속하기 위해 도구를 다운로드 받습니다.
     1. 아래 홈페이지에서 Putty를 다운로드 받습니다. 또는 익숙한 도구를 미리 설치 합니다.

|  |
| --- |
| <http://putty.org> |

* 1. 실습 비용 한도에 따른 유의 사항
     1. 실습을 종료 하고나서 가급적 사용하지 않는 서비스들은 삭제합니다. 불필요한 비용 발생으로 무료 구독이 중지되면 실습 진행이 어렵습니다.
     2. 고사양의 가상 컴퓨터나 서비스를 생성하지 않습니다. 고사양 서비스들은 고비용이 청구되어 단시간에 제공된 무료 구독의 비용을 초과할 수 있습니다.

1. 실습 전에 구성하고자하는 솔루션의 아키텍쳐를 소개 합니다.
   1. 전체 아키텍쳐는 다음과 같습니다.

|  |
| --- |
|  |

* 1. 진행 순서는, 우선 East Asia와 Southeast Asia간에 VPN 구성을 진행합니다. 각 리전별 VPN 구성에는 약 30분에서 45분이 소요될 수 있으므로 VPN 구성을 시작하고 나서, Japan West에 Windows Server 2012 R2 기반에 RRAS를 구성하여 시간 절약을 할 수 있도록 합니다.

1. East Asia에 Virtual Network를 구성합니다.
   1. 첫 번째 구성은 아래 그림에서와 같이 구성을 목적으로 합니다. 시간 절약을 위해서 Virtual Network 구성과 VPN 구성을 한 뒤에 각각 리전에 Virtual Machine을 생성하겠습니다.

|  |
| --- |
|  |

* 1. Azure Portal에서 Virtual Network를 선택합니다. Resource Manager가 선택 되었는지 확인하고 [Create]를 클릭하여 다음으로 진행합니다.

|  |
| --- |
|  |

* 1. 아래와같이 적절한 정보를 입력하고 [Pin to Dashboard]를 체크하고 [Create]를 클릭하여 생성을 시작합니다.

|  |  |  |
| --- | --- | --- |
|  | | |
| Name | vnet-1-hkg |  |
| Address Space | 10.1.0.0/16 |  |
| Subnet Name | Default |  |
| Subnet Address range | 10.1.0.0/24 |  |
| Subscription | AzurePass | (환경별로 다를 수있음) |
| Resource Group | vnet2vnet-hkg |  |
| Location | East Asia |  |

1. Southeast Asia에 Virtual Network를 생성합니다.
   1. Azure Portal에서 Virtual Network를 선택합니다. Resource Manager가 선택 되었는지 확인하고 [Create]를 클릭하여 다음으로 진행합니다.

|  |
| --- |
| C:\Users\hyssh\AppData\Local\Microsoft\Windows\INetCacheContent.Word\VNet2Vnet02.png |

* 1. 아래와같이 적절한 정보를 입력하고 [Pin to Dashboard]를 체크하고 [Create]를 클릭하여 생성을 시작합니다.

|  |  |
| --- | --- |
|  | |
| Name  Address Space  Subnet Name  Subnet Address range  Subscription  Resource Group  Location | vnet-2-sig  10.2.0.0/16  default  10.2.0.0/24  AzureFreePass  vnet2vnet-sig  Southeast Asia |

* 1. 두 개 Virtual Network을 생성하면 아래와 같이 두 개이 Virtual Network 리소스들을 확인할 수 있습니다.

|  |
| --- |
|  |

1. 각각 Virtual Network에 Gateway Subnet을 구성 합니다.
   1. Vnet-1-hkg 를 클릭하여 아래 그림과 같이 Virtual Network 화면이 보이도록 합니다.

|  |
| --- |
|  |

* 1. ‘Settings’에서 ‘Subnets’를 선택합니다.

|  |
| --- |
|  |

* 1. ‘+Gateway subnet’을 클릭하여 새로운 subnet 구성을 완료 합니다.

|  |
| --- |
|  |

* 1. [OK]를 클릭하고 아래와 같이 default 외Gateway subnet 이 생성되었는지 확인합니다.

|  |
| --- |
|  |

* 1. Vnet-2-sig 으로 명명된 Virtual Network를 선택하고 역시 subnet을 추가하여 아래와 같이 구성을 완료 합니다.

|  |
| --- |
|  |

1. Vnet-1-hkg에 Virtual Network Gateway를 생성합니다.
   1. Azure Portal에서 ‘Virtual Network Gateway’를 검색 합니다.

|  |
| --- |
|  |

* 1. 검색 결과 창에서 ‘Virtual Network Gateway’를 선택 합니다.

|  |
| --- |
|  |

* 1. [Create]를 클릭하여 생성 마법사를 시작합니다.

|  |
| --- |
|  |

* 1. 아래 그림에서 처럼 Location을 먼저 선택 합니다. 이번 순서에서는 East Asia를 선택 합니다. VPN 을 구분할 수 있는 이름을 명명합니다.

|  |
| --- |
|  |

* 1. ‘Virtual Network’를 클릭하여 ‘vnet-1-hkg’ virtual network를 클릭합니다.

|  |
| --- |
|  |

* 1. ‘Public IP address’를 클릭하고, ‘Create new’ 를 클릭하여 Virtual Network Gateway가 가지게될 public ip 주소를 새로 만듭니다.

|  |
| --- |
|  |

* 1. Public IP address를 구분할 수 있는 이름을 명명합니다.

|  |
| --- |
|  |

* 1. 아래와 같이 옵션 선택이 완료되었다면 [Pin to dashboard]에 체크하고 [Create]를 클릭하여 Virtual Network Gateway 생성을 시작 합니다. 생성에는 30분에서 45분이 소요 될 수 있습니다. 따라서 다음 ‘vnet-2-sig’에 Virtual Network Gateway 생성을 이어서 진행하도록 합니다.

|  |  |  |
| --- | --- | --- |
|  | | |
| Name | Hkg-vpn |  |
| Gateway Type | VPN |  |
| VPN Type | Route-based |  |
| SKU | Standard |  |
| Virtual Network | Vnet-1-hkg |  |
| Public IP address | Hkg-vpn-ip |  |
| Subscription | AzureFreePass | 환경에따라 다를 수 있음 |
| Resource group | Vent2vnet-hkg |  |
| Location | East Asia |  |

1. ‘Vnet-2-sig’에 Virtual Network Gateway를 구성 합니다.
   1. 새로운 서비스 만들기에서 ‘Virtual Network Gateway’를 검색하고 아래와 같이 서비스를 선택한 뒤 [Create]를 클릭하여 서비스 생성마법사를 시작합니다.

|  |
| --- |
|  |

* 1. ‘Location’을 Southeast Asia로 선택합니다.

|  |
| --- |
|  |

* 1. Virtual Network Gateway 의 이름을 명명하고 ‘Virtual Network’를 클릭하여 ‘Vnet-2-sig’를 선택 합니다.

|  |
| --- |
|  |

* 1. Virtual Network Gateway의 Public IP를 생성합니다. 적절한 이름을 명명합니다.

|  |
| --- |
|  |

* 1. 아래와 같이 옵션 선택이 완료되었다면 [Pin to dashboard]에 체크하고 [Create]를 클릭하여 Virtual Network Gateway 생성을 시작 합니다. 생성에는 30분에서 45분이 소요 될 수 있습니다.

|  |  |  |
| --- | --- | --- |
|  | | |
| Name | sig-vpn |  |
| Gateway Type | VPN |  |
| VPN Type | Route-based |  |
| SKU | Standard |  |
| Virtual Network | Vnet-2-sig |  |
| Public IP address | sig-vpn-ip |  |
| Subscription | AzureFreePass | 환경에따라 다를 수 있음 |
| Resource group | Vent2vnet-sig |  |
| Location | Southeast Asia |  |

* 1. 아래와같이 대시보드에서 두 개의 Virtual Network Gateway가 생성 중임을 확인 할 수 있습니다. 계속해서 각 Region에 배포된 Virtual Network에 Virtual Machine을 생성하여 두 Virtual Network간에 네트워크 구성이 올바르게 되었는지 확인 할 수 있도록 테스트용 Virtual Machine을 만들도록 합니다.

|  |
| --- |
|  |

1. Virtual Network Gateway가 생성되는동안 각 리전에 Virtual Machine을 생성합니다. 생성한 Virtual Machine을 사용해서 양쪽 Virtual Network간에 IPSec 터널링이 올바르게 구성되었는지 활용하는 용도로 사용 합니다.
   1. 새로운 서비스 만들기에서 ‘Ubuntu’를 검색하여 가상 컴퓨터 만들기 마법사를 시작합니다.
   2. 아래와 같이 ‘Resource Group’과 ‘Location’이 올바르게 선택되었는지 확인하고 [OK]를 클릭합니다. ‘vnet2vnet-hkg’와 ‘East Asia’가 선택되었는지 확인 합니다.

|  |
| --- |
|  |

* 1. 테스트용으로 ‘D1’을 선택합니다. 비용 절약을 위해서 가급적 1core 수준으로 선택하십시오.

|  |
| --- |
|  |

* 1. 아래와 같이 네트워크 정보에 ‘vnet-1-hkg’와 ‘default (10.1.0.0./24)’ 가 선택되었는지 확인하고 [OK]클릭합니다.

|  |
| --- |
|  |

* 1. 요약된 내용이 맞는지, 특히 네트워크 정보가 맞는지 확인하고 [OK]를 클릭하여 Virtual Machine 생성을 시작 합니다.

|  |
| --- |
|  |

1. Southeast Asia에 Virtual Machine을 생성합니다.
   1. 새로운 서비스 만들기에서 ‘Ubuntu’를 검색하여 가상 컴퓨터 만들기 마법사를 시작합니다.
   2. 아래와 같이 ‘Resource Group’과 ‘Location’이 올바르게 선택되었는지 확인하고 [OK]를 클릭합니다. 이번에는 ‘vnet2vnet-sig’와 ‘Southeast Asia’가 선택되었는지 확인 합니다.

|  |
| --- |
|  |

* 1. 테스트용으로 ‘D1’을 선택합니다. 비용 절약을 위해서 가급적 1core 수준으로 선택하십시오.

|  |
| --- |
|  |

* 1. 아래와 같이 네트워크 정보에 ‘vnet-2-sig’와 ‘default (10.2.0.0./24)’ 가 선택되었는지 확인하고 [OK]클릭합니다.

|  |
| --- |
|  |

* 1. 요약된 내용이 맞는지, 특히 네트워크 정보가 맞는지 확인하고 [OK]를 클릭하여 Virtual Machine 생성을 시작 합니다.

1. 두 개 Virtual Network Gateway와 Virtual Machine 생성이 완료되면 아래와 같이 대시보드에 서비스가 준비 되었음을 볼 수 있습니다.

|  |
| --- |
|  |

1. ‘hkg-vpn’으로 명명된 ‘East Asia’에 Virtual Network Gateway를 선택합니다.
   1. 클릭하면 아래와 같이 서비스 상태정보 창이 나타납니다. 올바르게 선택하셨는지 확인 합니다.

|  |
| --- |
|  |

* 1. ‘Settings’에 ‘Connections’를 선택 합니다.

|  |
| --- |
|  |

* 1. [+Add]를 클릭합니다.

|  |
| --- |
|  |

* 1. ‘Connection’을 구분할 수 있는 이름을 명명합니다. 이번 실습에서는 ‘hkg-to-sig’라고 명명하도록 합니다.

|  |
| --- |
|  |

* 1. ‘First virtual network gateway’는 hkg-vpn’으로 고정되어있습니다. ‘hkg-vpn’과 연결될 ‘Second Virtual network gateway’를 클릭하고 ‘sig-vpn’을 선택합니다.

|  |
| --- |
|  |

* 1. ‘Shared Key’에 ‘abcdef123456’을 입력합니다. 실제 프로덕션 환경에서는 복잡도가 높은 암호를 반드시 사용하도록 합니다.

|  |
| --- |
|  |

* 1. [OK]를 클릭하여 완료 합니다.

1. ‘sig-vpn’으로 명명된 ‘Southeast Asia’에 Virtual Network Gateway를 선택 합니다.
   1. 아래와 같이 ‘connections’ 이름을 명명하고 ‘Second virtual network gateway’를 선택합니다.

|  |
| --- |
|  |

* 1. ‘Shared Key’에 ‘abcdef123456’을 입력 합니다. 실제 프로덕션 환경에서는 복잡도가 높은 암호를 이용하도록 합니다.

|  |
| --- |
|  |

1. 10번과 11번 과정을 모두 거처야 ‘hkg-vpn’과 ‘sig-vpn’ 연결이 완료 됩니다.
   1. 두 VPN 간 연결 상태가 아래와같이 ‘Connected’ 인지 확인 합니다.

|  |
| --- |
|  |

* 1. 7번과 8번 과정에서 생성한 Virtual Machine 에 각각 접속합니다. 접속을 위해서는 미리 다운로드 받은 putty를 이용하여 Public IP로 접속합니다. 각각 VM에 접속하여 사설 IP 주소로 ping이 되는지 확인하도록 합니다
     1. Hkg1에서는 10.2.0.4번으로 ping 테스트 합니다.
     2. Sig1에서는 10.1.0.4번으로 ping 테스트 합니다.

1. 지금부터는, 아래 그림에서, Japan West 를 구성 합니다.

|  |
| --- |
|  |

* 1. Azure Virtual Network Gateway와 on-premise VPN 장비와 연결 테스트를 하기위해서 Windows Server 2012 에 RRAS를 Azure에 구성합니다. RRAS 구성을 위해서는 최소 2개의 NIC이 장착된 가상 컴퓨터가 필요합니다. 따라서 준비된 ARM Template를 통해 Japan West에 Virtual Machine을 생성하여 이를 RRAS로 구성합니다.
  2. 아래는 이번 실습을 위해 준비한 ARM Template입니다. Azure Portal에 로그인이 되어있는 상태에서 아래 주소를 IE (또는 웹브라우저)를 통해 접속 합니다.

|  |
| --- |
| <https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fwebinarhub.blob.core.windows.net%2Fazurehol%2FWin_RRAS_azuredeploy.json> |

* 1. 아래와 같이 custom template에 파라미터를 입력하여 NIC이 2개 장착된 Windows Server 2012를 구성합니다. ‘Resource Group’에는 ‘vnet-3-jpw’를 입력 합니다. ‘Virtual Machines\_winvpn\_adminPassword’에 적당한 Windows 의 암호를 입력하고 본 서버의 디스크가 저장될 Storage account이름을 ‘Storage Account\_aznetworkinghkgdisks578\_name’에 입력합니다.

|  |
| --- |
|  |

* 1. 아래와 같이 ‘I agree to the terms and conditions stated above’와 ‘Pin to dashboard’에 체크박스 체크 후 [Purchase]를 클릭하여 Windows Server 2012 R2를 생성합니다.

|  |
| --- |
|  |

* 1. 해당 template 배포에는 10분 미만이 소요되며, 배포가 완료되면 아래와 같이 구성 정보를 확인 할 수 있습니다. ‘vnet-3-jpw’으로 명명된 Virtual Network은 10.3.0.0/16 주소 영역을 갖고 있습니다.

|  |
| --- |
|  |

1. ‘hkg-vpn’과 Widows Server 2012 R2 RRAS와 연결을 해보도록 합니다.
   1. Azure쪽 VPN에 ‘win-rras’의 연결 (Connection)정보를 입력합니다. 아래 대시보드에서 ‘hkg-vpn’을 선택 합니다.

|  |
| --- |
|  |

* 1. ‘Settings’에서 ‘Connections’를 선택합니다. 아래와 같이 기존 연결되 2개의 connections를 확인 할 수 있습니다. 여기에 추가로 ‘win-rras’를 입력합니다.

|  |
| --- |
|  |

* 1. [+Add]를 클릭합니다. 아래 그림과 같이 ‘Connection Type’을 ‘Site-to-Site (IPSec)’를 선택 합니다.

|  |
| --- |
|  |

* 1. ‘Connection’을 구분할 수 있는 이름을 명명합니다. 이번 실습에서는 ‘hkg-to-jpw’라고 명명합니다.

|  |
| --- |
|  |

* 1. ‘Local network gateway’를 클릭합니다.

|  |
| --- |
|  |

* 1. 새로운 ‘Local network gateway’를 생성하기 위한 정보를 입력 합니다. IP Address는 13번에서 생성한 Windows Server의 Public IP Address를 입력합니다. 그리고 Japan West에서 사용중인 Address Space 를 입력합니다.

|  |
| --- |
|  |

* 1. ‘Shared Key (PSK)’ 를 입력 합니다. [OK]를 클릭하고 ‘Connection’ 생성을 완료 합니다. 이로서 ‘hkg-vpn’은 ‘win-rras’에 대한 연결정보를 얻게 되었습니다. 양방향 IPSec을 위해서는 ‘win-rras’가 ‘hkg-vpn’에 대한 정보를 알 수 있도록 계속 진행합니다.

|  |
| --- |
|  |

1. Windows Server 2012 R2 에서 RRAS를 설치 합니다.
   1. ‘win-rras’에 접속 (connect) 합니다 .

|  |
| --- |
|  |

* 1. 원활한 테스트를 위해 우선 ‘win-rras’에 윈도우즈 방화벽 서비스를 종료 합니다. 실제 프로덕션에서는 적절한 방화벽 구성이 강력히 권장됩니다.

|  |
| --- |
|  |

* 1. ‘win-rras’ 에 원격 데스크탑으로 접속한 아래 PowerShell명령으로 RRAS를 설치 합니다. VM 사양에 따라 몇 분 정도 소요될 수 있습니다.

|  |
| --- |
| **Import-Module ServerManager**  **Install-WindowsFeature RemoteAccess -IncludeManagementTools**  **Add-WindowsFeature -name Routing -IncludeManagementTools**  **Import-Module RemoteAccess**  **if ((Get-RemoteAccess).VpnS2SStatus -ne "Installed")**  **{**  **Install-RemoteAccess -VpnType VpnS2S**  **}** |

1. RRAS 설치가 완료되면 ‘hkg-vpn’과 연결될 수 있도록 ‘hkg-vpn’정보를 추가하고 연결 합니다.
   1. RRAS를 실행합니다. 아래 그림에서처럼 ‘Server Manager’ > ‘Tools’ > ‘Routing and Remote Access’를 실행합니다.

|  |
| --- |
|  |

* 1. ‘Network Interfaces’에서 마우스 오른쪽 클릭하여 ‘New Demand-dial Interface…’를 클릭합니다.

|  |
| --- |
|  |

* 1. Interface를 구분하는 이름을 입력합니다. Azure에 ‘hkg-vpn’과 연결할 것이므로 이름을 ‘azure-hkg’로 입력합니다. 그리고 ‘Next’를 클릭하여 다음으로 넘어갑니다.

|  |
| --- |
|  |

* 1. 연결 타입은 VPN을 선택합니다. 그리고 ‘Next’를 클릭하여 다음으로 넘어갑니다.

|  |
| --- |
|  |

* 1. VPN 타입은 IKEv2를 선택합니다. 그리고 ‘Next’를 클릭하여 다음으로 넘어갑니다.

|  |
| --- |
|  |

* 1. VPN 목적지의 주소입니다. 이번 실습 단계에서는 Azure에 ‘hkg-vpn’과 연결하는 것으로 ‘hkg-vpn’의 public ip를 입력하도록 합니다. Ip 주소가 틀리면 연결에 실패 할 수 있으므로 정확한 주소 입력이 요구 됩니다. 입력후 ‘Next’를 클릭하여 다음으로 넘어갑니다.

|  |
| --- |
|  |

* 1. 프로토콜과 보안 관련 옵션에는 첫 번째 ‘Route IP packets on this interface’만 선택합니다. 그리고 ‘Next’를 클릭하여 다음으로 넘어갑니다.

|  |
| --- |
|  |

* 1. ‘hkg-vpn’을 통해 통신할 원격지의 주소 대역을 입력합니다. ‘Add’를 클릭하여 주소를 입력 합니다.

|  |
| --- |
|  |

* 1. ‘hkg-vpn’에 연결된 네트워크 주소는 10.1.0.0/16 입니다. 아래와 같이 목적지 주소와 네트워크 마스크 정보를 입력합니다. Metric에는 적절한 정보를 입력합니다. ‘OK’를 클릭하여 추가를 완료 합니다.

|  |
| --- |
| ' |

* 1. 정확한 정보가 입력되었는지 확인하고 ‘Next’를 클릭하여 다음으로 넘어갑니다.

|  |
| --- |
|  |

* 1. Dial-Out Credentials는 이번 실습에서 불필요하므로 공란으로 두고 ‘Next’를 클릭하여 다음으로 넘어갑니다.

|  |
| --- |
|  |

* 1. ‘Finish’를 클릭하여 마법사를 완료 합니다.

|  |
| --- |
|  |

* 1. 본 실습에서는 IKEv2방식으로 VPN 간 연결이 되어야 합니다. 따라서 지금 추가한 네트워크 인터페이스에 ‘hkg-vpn’과 동일한 ‘preshared key’를 입력 해야합니다. 방금 추가한 네트워크 인터페이스 이름 위에서 마우스 오른쪽을 클릭하여 ‘Property’를 클릭합니다.

|  |
| --- |
|  |

* 1. ‘Security’ 탭을 클릭합니다.

|  |
| --- |
|  |

* 1. ‘Security’ 탭에서 pre-shared key를 입력 하고 ‘OK’를 클릭하여 완료 합니다.

|  |
| --- |
|  |

* 1. Pre-shared key가 추가 되었으므로 VPN간 연결 준비가 끝났습니다. 네트워크 인터페이스에서 마우스 오른쪽을 클릭하여 ‘Connect’를 클릭합니다. Azure와 ‘win-rras’간 연결이 되었는지 ping 테스트를 수행합니다.

|  |
| --- |
|  |

모든 실습이 종료되었습니다. 불필요한 서비스를 삭제하여 비용 지출을 최소화 하도록 합니다.