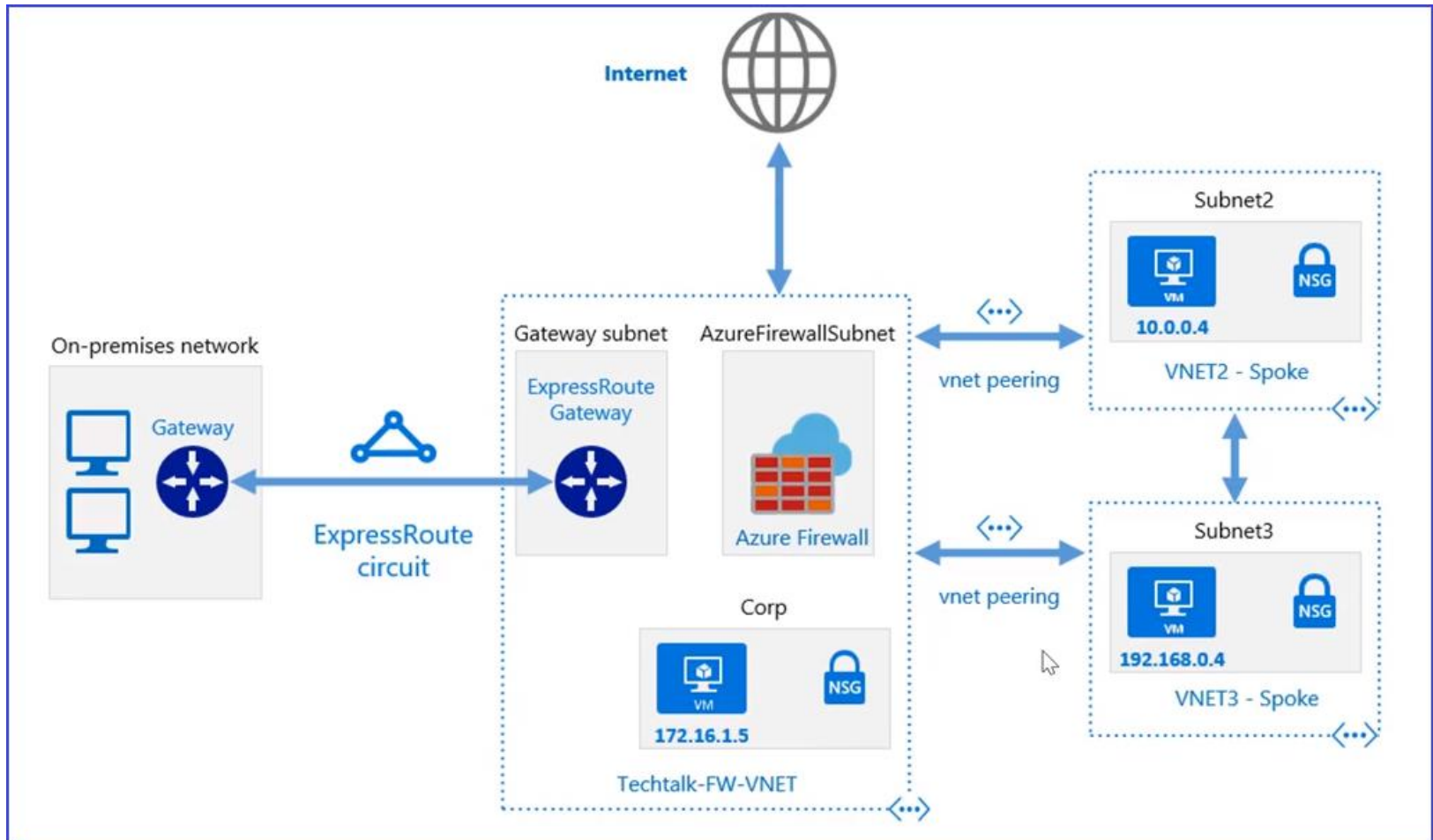


# Azure Firewall 설정하기

- VNet 구성 및 Firewall 구성도
  - 참고 동영상: [https://youtu.be/g6tl\\_EU0rnU](https://youtu.be/g6tl_EU0rnU)



# Azure Firewall 설정하기

- Azure Firewall 개요
  - 참고:<http://techtalk.cloud/azure-firewall/> (강추)
  - Microsoft's full managed, scalable Firewall as a Service
  - Provides SNAT and DNAT Support
  - Filter inbound/Outbound traffic across
    - VNets (Hub and Spoke)
    - On-Premises Network
    - Internet
  - Provides Centralized Logging

# Azure Firewall 설정하기

- Azure Firewall 설정 순서
  - 3개의 VNet 생성하기
    - VNet-FW(172.16.1.0/24:Corp 서브넷)
    - VNet-2(10.0.0.0/24: Subnet2 서브넷)
    - VNet-3(192.168.0.0/24: Subnet3 서브넷)
  - 3개의 VM 생성하기
    - VM-FW, VM-2, VM-3
    - 각 VNet/Subnet에 VM 배포하기
  - VNet간에 Network Peering 구성하기
    - VM-FW <-> VM-2
    - VM-FW <-> VM-3
  - Azure Firewall 생성하기
    - myFW
  - Firewall에 사용할 Route Table **생성하기**
    - RT-FW

# Azure Firewall 설정하기

- Azure Firewall 설정 순서
  - Firewall Rule 생성하기
    - DNAT Rule(Port Forwarding)을 구성하여 incoming RDP Request 허용하기
    - NAT Rule을 구성하여 VNet과 Subnet간에 Allow/Disallow 연결하기
  - Diagnostic logging 사용하기

# Azure Firewall 설정하기

- 3개의 VNet 생성하기
  - VNet-FW(172.16.1.0/24:Corp 서브넷)
  - VNet-2(10.0.0.0/24: Subnet2 서브넷)
  - VNet-3(192.168.0.0/24: Subnet3 서브넷)

Create virtual network ☐

\* Name  
VNet-FW ✓

\* Address space ⓘ  
172.16.0.0/16 ✓  
172.16.0.0 - 172.16.255.255 (65536 addresses)

\* Subscription  
Azure Pass - 스폰서쉽 ▼

\* Resource group  
myRG ▼  
[Create new](#)

\* Location  
(US) East US ▼

Subnet

\* Name  
Corp ✓

\* Address range ⓘ  
172.16.1.0/24 ✓  
172.16.1.0 - 172.16.1.255 (256 addresses)

Create virtual network ☐

\* Name  
VNet-2 ✓

\* Address space ⓘ  
10.0.0.0/16 ✓  
10.0.0.0 - 10.0.255.255 (65536 addresses)

\* Subscription  
Azure Pass - 스폰서쉽 ▼

\* Resource group  
myRG ▼  
[Create new](#)

\* Location  
(US) East US ▼

Subnet

\* Name  
Subnet-2 ✓

\* Address range ⓘ  
10.0.0.0/24 ✓  
10.0.0.0 - 10.0.0.255 (256 addresses)

Create virtual network ☐

\* Name  
VNet-3 ✓

\* Address space ⓘ  
192.168.0.0/16 ✓  
192.168.0.0 - 192.168.255.255 (65536 addresses)

\* Subscription  
Azure Pass - 스폰서쉽 ▼

\* Resource group  
myRG ▼  
[Create new](#)

\* Location  
(US) East US ▼

Subnet




\* Name  
Subnet-3 ✓

\* Address range ⓘ  
192.168.0.0/24 ✓  
192.168.0.0 - 192.168.0.255 (256 addresses)

# Azure Firewall 설정하기

- 3개의 VM 생성하기

- Windows Server 2016(Standard B2s), adminuser(P@ssw0rd1234)
- RDP만 허용
- VM-FW
  - VNet-FW에 연결 / ysleevmfw.eastus.cloudapp.azure.com
- VM-2
  - VNet-2에 연결 / ysleevm2.eastus.cloudapp.azure.com
- VM-3
  - VNet-3에 연결 / ysleevm3.eastus.cloudapp.azure.com

<input type="checkbox"/>	NAME <small>↑↓</small>	STATUS	RESOURCE GROUP <small>↑↓</small>	LOCATION <small>↑↓</small>	PRIVATE IP ADDRESS	PUBLIC DNS NAME
<input type="checkbox"/>	 VM-2	Running	myRG	East US	10.0.0.4	ysleevm2.eastus.cloudapp.azure.com
<input type="checkbox"/>	 VM-3	Running	myRG	East US	192.168.0.4	ysleevm3.eastus.cloudapp.azure.com
<input type="checkbox"/>	 VM-FW	Running	myRG	East US	172.16.1.4	ysleevmfw.eastus.cloudapp.azure.com

# Azure Firewall 설정하기

- VNet간에 Network Peering 구성하기
  - VM-FW <-> VM-2

### Add peering

VNet-FW

---

\* Name of the peering from VNet-FW to VNet-2

VNetFW\_VNet2

---

#### Peer details

Virtual network deployment model ⓘ

☒ Resource manager ☐ Classic

☐ I know my resource ID ⓘ

\* Subscription ⓘ

Azure Pass - 스폰서쉽

\* Virtual network

VNet-2 (myRG)

---

#### Configuration

Configure virtual network access settings

Allow virtual network access from VNet-FW to VNet-2 ⓘ

☐ Disabled ☒ Enabled

Configure forwarded traffic settings

Allow forwarded traffic from VNet-FW to VNet-2 ⓘ

☐ Disabled ☒ Enabled

### Add peering

VNet-2

---

\* Name of the peering from VNet-2 to VNet-FW

VNet2\_VNetFW

---

#### Peer details

Virtual network deployment model ⓘ

☒ Resource manager ☐ Classic

☐ I know my resource ID ⓘ

\* Subscription ⓘ

Azure Pass - 스폰서쉽

\* Virtual network

VNet-FW (myRG)

---

#### Configuration

Configure virtual network access settings

Allow virtual network access from VNet-2 to VNet-FW ⓘ

☐ Disabled ☒ Enabled

Configure forwarded traffic settings

Allow forwarded traffic from VNet-2 to VNet-FW ⓘ

☐ Disabled ☒ Enabled

# Azure Firewall 설정하기

- VNet간에 Network Peering 구성하기
  - VM-FW <-> VM-3

### Add peering

VNet-FW

\* Name of the peering from VNet-FW to VNet-3

VNetFW\_VNet3

#### Peer details

Virtual network deployment model ⓘ

☒ Resource manager ☐ Classic

☐ I know my resource ID ⓘ

\* Subscription ⓘ

Azure Pass - 스폰서쉽

\* Virtual network

VNet-3 (myRG)

#### Configuration

Configure virtual network access settings

Allow virtual network access from VNet-FW to VNet-3 ⓘ

☐ Disabled ☒ Enabled

Configure forwarded traffic settings

Allow forwarded traffic from VNet-FW to VNet-3 ⓘ

☐ Disabled ☒ Enabled

### Add peering

VNet-3

\* Name of the peering from VNet-3 to VNet-FW

VNet3\_VNetFW

#### Peer details

Virtual network deployment model ⓘ

☒ Resource manager ☐ Classic

☐ I know my resource ID ⓘ

\* Subscription ⓘ

Azure Pass - 스폰서쉽

\* Virtual network

VNet-FW (myRG)

#### Configuration

Configure virtual network access settings

Allow virtual network access from VNet-3 to VNet-FW ⓘ

☐ Disabled ☒ Enabled

Configure forwarded traffic settings

Allow forwarded traffic from VNet-3 to VNet-FW ⓘ

☐ Disabled ☒ Enabled



# Azure Firewall 설정하기

- VNet간에 Network Peering 구성하기
  - Network Peering를 구성하였기 때문에 VM간에 통신 여부 확인하기
  - mstsc.exe로 각 VM에 접속하기
  - 각 VM에서 firewall.cpl을 실행하여 윈도우 방화벽 기능을 끄기
  - VM-FW에서 VM-2(10.0.0.4)로 Ping 통신 **(##성공)**
  - VM-FW에서 VM-3(192.168.0.4)로 Ping 통신 **(##성공)**
  - VM-2에서 VM-FW(172.16.1.4)로 Ping 통신 **(##성공)**
  - VM-3에서 VM-FW(172.16.1.4)로 Ping 통신 **(##성공)**
  - VM-3에서 VM-2(10.0.0.4)로 Ping 통신 **(##실패)**

# Azure Firewall 설정하기

- Azure Firewall 생성하기
  - VNet-FW에 서브넷 AzureFirewallSubnet(172.16.0.0/24) 생성하기(필수)

Home > Virtual networks > VNet-FW - Subnets > Add subnet

### Add subnet

VNet-FW

\* Name

AzureFirewallSubnet

\* Address range (CIDR block) ⓘ

172.16.0.0/24

172.16.0.0 - 172.16.0.255 (251 + 5 Azure reserved addresses)

### VNet-FW - Subnets

Virtual network

Search (Ctrl+/)

+ Subnet + Gateway subnet

Search subnets

NAME	ADDRESS RANGE	AVAILABLE ADDRE...
Corp	172.16.1.0/24	250
AzureFirewallSubnet	172.16.0.0/24	251

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

# Azure Firewall 설정하기

- Azure Firewall 생성하기
  - Firewall 이름: myFW
  - 사설 IP와 공인 IP 확인

Virtual network/subnet : VNet-FW/AzureFirewallSubnet

Private IP address : 172.16.0.4

Public IP address : azureFirewalls-ip

Provisioning state : Succeeded



SKU : Standard

IP address : 52.191.217.172

DNS name : -

Associated to : myFW

Virtual machine : -

## PROJECT DETAILS

\* Subscription

Azure Pass - 스폰서쉽

\* Resource group

myRG

[Create new](#)

## INSTANCE DETAILS

\* Name

myFW

\* Region

(US) East US

Choose a virtual network

☐ Create new ☒ Use existing

Virtual network

VNet-FW (myRG)

## PUBLIC IP ADDRESS

\* Public IP address ⓘ

☒ Create new ☐ Use existing

\* Public IP address name

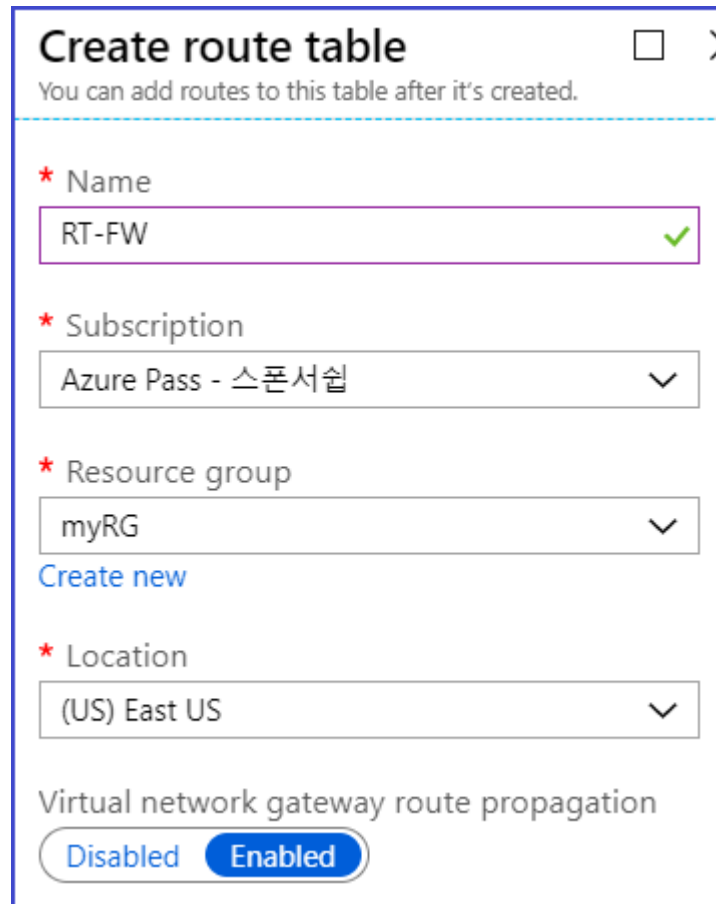
azureFirewalls-ip

Public IP address SKU

Standard

# Azure Firewall 설정하기

- Firewall에 사용할 Route Table **생성하기**
  - 이름: RT-FW



The screenshot shows the 'Create route table' form in the Azure portal. The form is titled 'Create route table' with a subtitle 'You can add routes to this table after it's created.' Below the title, there are four required fields marked with a red asterisk: 'Name' (containing 'RT-FW' with a green checkmark), 'Subscription' (containing 'Azure Pass - 스폰서쉽'), 'Resource group' (containing 'myRG'), and 'Location' (containing '(US) East US'). Below these fields is a link 'Create new'. At the bottom, there is a section for 'Virtual network gateway route propagation' with two buttons: 'Disabled' and 'Enabled' (which is selected).

**Create route table** ☐ >

You can add routes to this table after it's created.

\* Name  
RT-FW ✓

\* Subscription  
Azure Pass - 스폰서쉽 ▼

\* Resource group  
myRG ▼

[Create new](#)

\* Location  
(US) East US ▼

Virtual network gateway route propagation

# Azure Firewall 설정하기

- Firewall에 사용할 Route Table 구성하기
  - Route 추가하기

RT-FW - Routes  
Route table

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems

Settings

Configuration  
Routes  
Subnets

Search routes

NAME

No results.

+ Add

NAME	ADDRESS PREFIX	NEXT HOP
Route-FW	0.0.0.0/0	172.16.0.4
RouteToProduction	172.16.0.0/16	172.16.0.4
RouteToVNet2	10.0.0.0/16	172.16.0.4
RouteToVNet3	192.168.0.0/16	172.16.0.4

# Azure Firewall 설정하기

- Firewall에 사용할 Route Table 구성하기
  - Route 추가하기

<b>Add route</b>	
RT-FW	
* Route name	Route-FW
* Address prefix ⓘ	0.0.0.0/0
Next hop type ⓘ	Virtual appliance
* Next hop address ⓘ	172.16.0.4

<b>Add route</b>	
RT-FW	
* Route name	RouteToProduction
* Address prefix ⓘ	172.16.0.0/16
Next hop type ⓘ	Virtual appliance
* Next hop address ⓘ	172.16.0.4

<b>Add route</b>	
RT-FW	
* Route name	RouteToVNet2
* Address prefix ⓘ	10.0.0.0/16
Next hop type ⓘ	Virtual appliance
* Next hop address ⓘ	172.16.0.4

<b>Add route</b>	
RT-FW	
* Route name	RouteToVNet3
* Address prefix ⓘ	192.168.0.0/16
Next hop type ⓘ	Virtual appliance
* Next hop address ⓘ	172.16.0.4



Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

# Azure Firewall 설정하기

- Firewall Rule 생성하기
  - **NAT** Rule Collection 구성하기
    - DNAT Rule(Port Forwarding)을 구성하여 incoming RDP Request 허용하기

Home > Firewalls > myFW - Rules

### Firewalls

기본 디렉터리

+ Add Edit columns More

Filter by name...

NAME ↑↓

myFW

### myFW - Rules

Firewall

Search (Ctrl+ /)

Overview  
Activity log  
Access control (IAM)  
Tags

Settings

Rules

Threat intelligence

Refresh

NAT rule collection Network rule collection Application rule collection

+ Add NAT rule collection

PRIORITY	NAME	ACTION	RULES
No results			

When a DNAT rule is matched, an implicit corresponding network rule to allow the translated traffic is created. [more.](#)

# Azure Firewall 설정하기

- Firewall Rule 생성하기
  - **NAT** Rule Collection 구성하기
    - DNAT Rule(Port Forwarding)을 구성하여 incoming RDP Request 허용하기

\* Name

\* Priority

\* Action  **mstsc.exe를 사용하여 52.191.217.172:9191로 접속하면 VM-FW(172.16.1.4)의 원격 데스크톱으로 접속을 허용한다**

Rules

NAME	PROTOCOL	SOURCE ADDRESSES	DESTINATION ADDRE...	DESTINATION PORTS	TRANSLATED ADDRESS	TRANSLATED PORT
RDP from Internet ✓	TCP ▼	* ✓	52.191.217.172 ✓	9191 ✓	172.16.1.4 ✓	3389 ✓

- 로컬 컴퓨터에서 Azure Firewall의 공인 IP의 9191 포트 번호로 접속을 시도하면 그 뒤에 있는 VM-FW에 원격 데스크톱에 접속하도록 설정한 것이다
- Azure Firewall이 Reverse Proxy 역할을 하는 것이다
- VM-FW의 Public IP를 제거한다
- mstsc.exe를 사용하여 Azure Firewall의 Public IP를 사용하여 VM-FW에 접속한다 (##성공)



# Azure Firewall 설정하기

- Firewall Rule 생성하기

- **Network** Rule Collection 구성하기

- Internet에서 Azure Firewall이 있는 VNet-FW 네트워크에 존재하는 VM에만 접속을 허용하고 Vnet-2, Vnet-3에 있는 VM에는 Internet으로부터의 접속을 허용하지 않는다
    - 이를 위해 Azure Firewall이 속한 Network(VNet-FW)에서만 Peering을 하고 있는 Vnet-2, Vnet-3에 3389로 접속할 수 있도록 구성한다
    - VM-2, VM-3의 **Public IP**는 제거한다. 그러면 Internet으로부터 3389 접속을 할 수 없다

PRIORITY	NAME	ACTION	RULES
No results			

# Azure Firewall 설정하기

- Firewall Rule 생성하기

- **Network** Rule Collection 구성하기

- Internet에서 직접 Vnet-2, Vnet-3의 VM에 접속은 불허하고, Vnet-FW에서 운영중인 VM에서만 Vnet-2, Vnet-3에 3389로 접속할 수 있다

## Add network rule collection

\* Name

\* Priority

\* Action

### Rules

#### IP Addresses

**172.16.0.0/16에 있는 VM에서만 10.0.0.0/16의 VM과 192.168.0.0/16에 있는 VM에 3389로 접속 허용함**

NAME	PROTOCOL	SOURCE ADDRESSES	DESTINATION ADDRESSES	DESTINATION PORTS
Allow-RDP-VNet2	Any	172.16.0.0/16	10.0.0.0/16	3389
Allow-RDP-VNet3	Any	172.16.0.0/16	192.168.0.0/16	3389

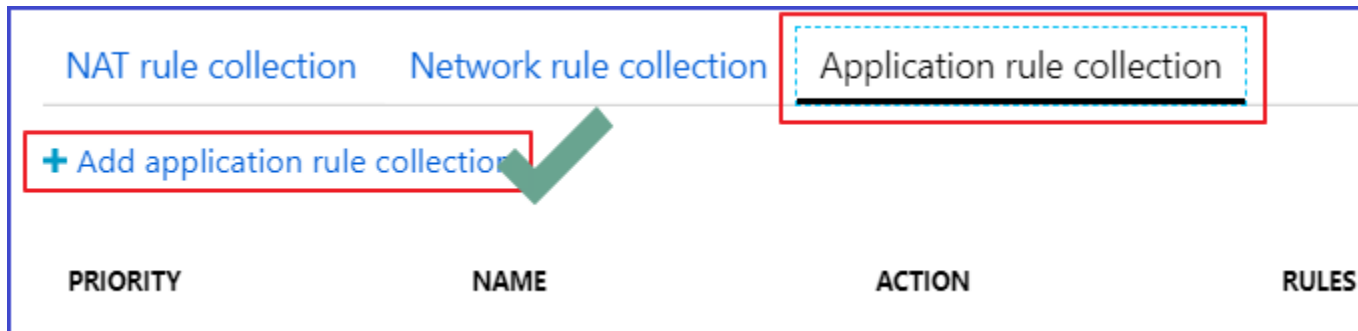
- VM-FW에서 VM-2, VM-3에 원격 데스크톱으로 연결한다(##성공)
- VM-3에서 ping 172.16.1.4(VM-FW)는 ttl이 128, ping 172.16.0.4(Azure Firewall)는 ttl 64가 나온다

# Azure Firewall 설정하기

- Firewall Rule 생성하기

- **Application** Rule Collection 구성하기

- Vnet-2, Vnet-3에 있는 VM에서 특정한 Internet web site에 접속하는 것을 차단하기
    - Vnet-2, Vnet-3에 있는 VM에서 Windows update는 허용하기



# Azure Firewall 설정하기

- Firewall Rule 생성하기
  - **Application** Rule Collection 구성하기

### Add application rule collection

★ Name

100

★ Priority

100


★ Action

Allow

Rules

FQDN tags

NAME	SOURCE ADDRESSES	FQDN TAGS
All Network allowed to Windows update ✓	172.16.0.0/24 ✓	WindowsUpdate
	*, 192.168.10.1, 192.168.10.0/24, 192.168.10.2 – 192.168.1...	0 selected

 FQDN tags may require additional configuration. [Learn more.](#)

Target FQDNs

NAME	SOURCE ADDRESSES	PROTOCOL:PORT	TARGET FQDNS
Allow Microsoft	*	http:80,https:443	*.microsoft.com
Allow Google	*	http:80,https:443	*.google.com
Allow Github ✓	* ✓	http:80,https:443 ✓	*.github.com ✓

# Azure Firewall 설정하기

- Diagnostic logging 사용하기
  - 미리 storage account가 생성되어 있어야 함
  - Azure Firewalls - Diagnostic Settings - Turn on diagnostics 선택

Turn on diagnostics to collect the following data.

- AzureFirewallApplicationRule
- AzureFirewallNetworkRule
- AllMetrics

**Diagnostics settings**

Save Discard Delete

\* Name  
AZ\_Firewalls\_logs ✓

☒ Archive to a storage account

Storage account  
ysleesa >

☐ Stream to an event hub

☐ Send to Log Analytics

**LOG**

<input checked="" type="checkbox"/> AzureFirewallApplicationRule	Retention (days) ⓘ <input type="range"/> 7
<input checked="" type="checkbox"/> AzureFirewallNetworkRule	Retention (days) ⓘ <input type="range"/> 7

**METRIC**

<input checked="" type="checkbox"/> AllMetrics	Retention (days) ⓘ <input type="range"/> 7
--	---