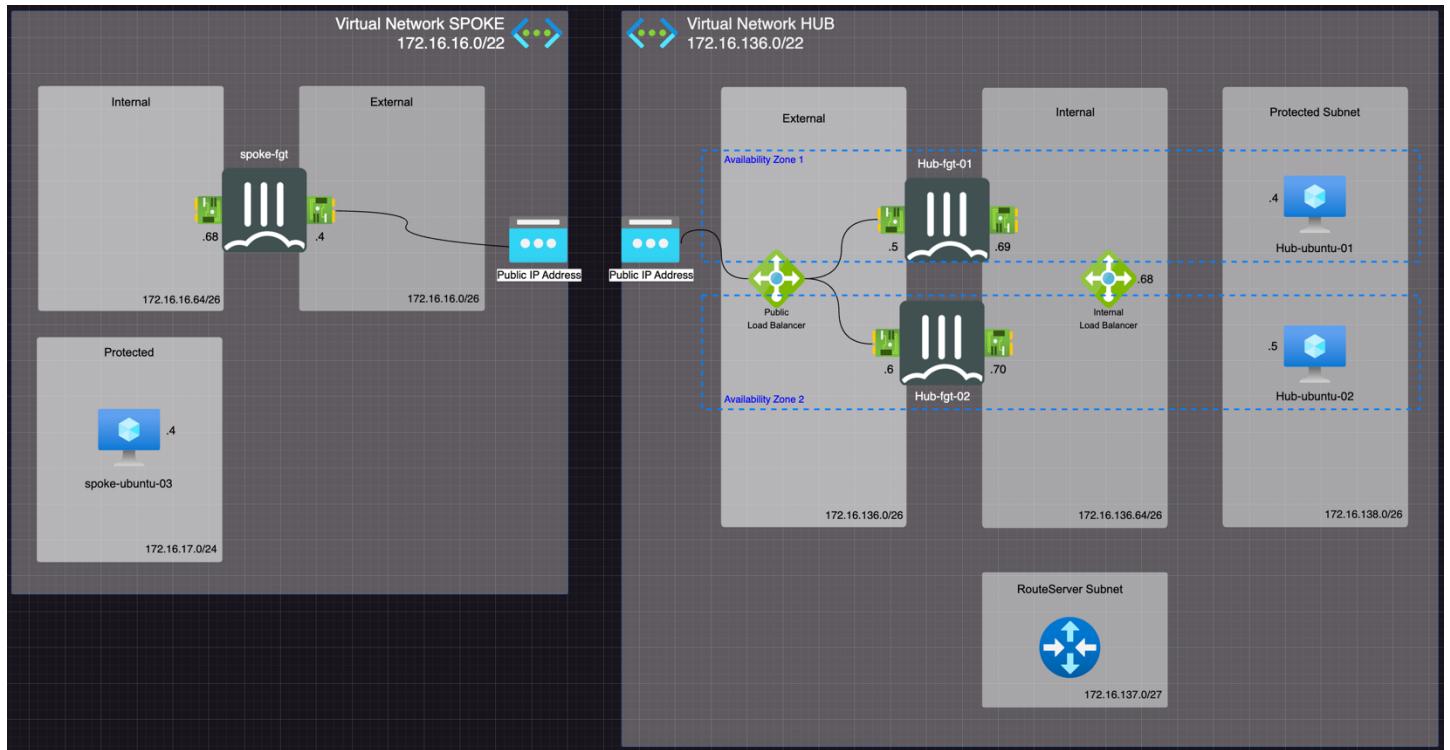


# Fortigate @AZURE lab

1.	<i>Creazione Resource Group</i>	3
2.	<i>HUB - Creazione cluster Fortigate Active/Active</i>	5
3.	<i>HUB - Creazione Azure Route Server</i>	8
4.	<i>HUB - Creazione server Ubuntu01</i>	11
5.	<i>HUB - Accesso server Ubuntu01 tramite VIP cluster</i>	13
	TEST	16
6.	<i>SPOKE - Creazione Fortigate single-vm</i>	17
7.	<i>SPOKE - Creazione server Ubuntu03</i>	20
8.	<i>SPOKE - Accesso server Ubuntu03 tramite VIP Fortigate spoke</i>	22
9.	<i>Configurazione BGP all'interno della vnet HUB</i>	24
	TEST	25
10.	<i>Configurazione VPN tra HUB e SPOKE</i>	27
10.1.	creazione regole di load balancing	27
10.2.	configurazione ipsec sui fortigate hub	28
10.3.	configurazione interfaccia ipsec sui fortigate hub	28
10.4.	configurazione bgp sui fortigate hub	29
10.5.	configurazione secondary ip address sui fortigate hub	29
10.6.	creazione regola sui fortigate hub	29
10.7.	configurazione ipsec su fortigate spoke	29
10.8.	configurazione interfaccia ipsec su fortigate spoke	30
10.9.	configurazione bgp su fortigate spoke	30
10.10.	creazione regola su fortigate spoke	30
	TEST	30
	TEST	31
11.	<i>HUB - Microsegmentazione</i>	33
	Installazione di un nuovo server hub-ubuntu-02	33
	Creazione e configurazione nuova routing table	36
	TEST	38
	Creazione policy per traffico EST-OVEST	39
	TEST	39
12.	<i>Segmentazione con VNET Peering</i>	40
12.1.	Creazione nuova VNET son una subnet Protected	40
12.2.	Creazione nuove VM all'interno delle nuove VNET	43
12.3.	Creazione nuova Route Table da associare alle nuove Subnet	46
12.4.	Configurazione VNET Peering	48
12.5.	Impostare il routing sui due Fortigate HUB	50
12.6.	TEST	51
13.	<i>Rimozione risorse</i>	52



# 1. Creazione Resource Group

Dalla home del portale Azure -> **Create a Resource**

The screenshot shows the Microsoft Azure home page. At the top, there's a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, there's a section titled "Azure services" containing several icons and links:

- Create a resource** (with a plus sign icon)
- Resource groups** (with a cube icon)
- Marketplace** (with a cloud icon)
- Microsoft Entra ID** (with a blue diamond icon)
- Tenant properties** (with a gear icon)
- Cost Management ...** (with a dollar sign icon)
- Subscriptions** (with a key icon)
- App Services** (with a globe icon)

Below these icons, there's a link to "Deployment Scripts" (with a script icon) and a large blue arrow pointing right labeled "More services".

Nel campo search digitare **resource group** e dare invio

The screenshot shows the Microsoft Azure Marketplace search results for "resource group". The search bar at the top contains the query "resource group". The results list shows one item:

- Resource group** (by Microsoft, Azure Service, Manage and deploy resources in an application together)

Below the results, there are sections for "Get Started", "Management", and "My Marketplace". The "Get Started" section has a "Create" button. The "Management" section includes links for "Private Marketplace", "Private Offer Management", and "Favorites". The "My Marketplace" section includes links for "My solutions", "Recently created", and "Private plans". The "Categories" section shows a list of categories, with "DevOps (82)" being the first item.

**Create Resource Group**

# Create a resource group

Basics Tags Review + create

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

## Project details

Subscription \* ⓘ

SE-Subscription

Resource group \* ⓘ

abcd22

## Resource details

Region \* ⓘ

(Europe) Italy North

Selezionare la Subscription

Nel campo Resource group (nome) inserire le iniziali Nome Cognome di entrambi i partecipanti + un numero a piacere

Region: Italy North

**Review + create -> Create**

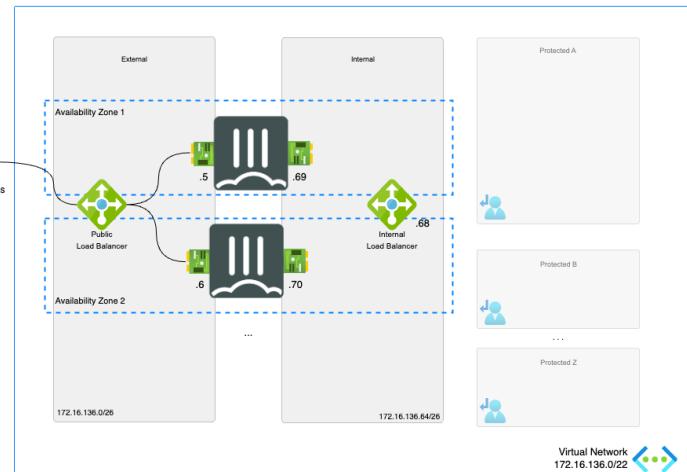
## 2. HUB - Creazione cluster Fortigate Active/Active

Per il deployment del cluster utilizzare il template ARM sul repository github

<https://github.com/caliaf/AZURE/edit/main/FortiGate/Active-Active-ELB-ILB/>

Copiare il link e incollarlo in un nuovo tab dello stesso browser con cui si è acceduti alla console di Azure per creare precedentemente il resource group.

Il template permette la configurazione di diverse opzioni per indirizzare molteplici architetture Active/Active.



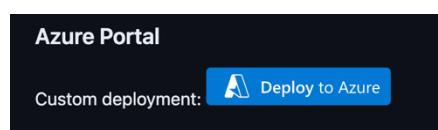
Per il laboratorio verrà creata un'infrastruttura con bilanciatore pubblico e bilanciatore privato

**Active/Active loadbalanced pair of standalone FortiGates for resilience and scale**

[FGT] ARM - Active-Active-ELB-ILB passing

👉 - [Introduction](#) - [Design](#) - [Deployment](#) - [Requirements](#) - [Configuration](#) - 👈

Nel menu del repository in alto sotto il titolo selezionare **Deployment**



Selezionare **Deploy to Azure**

Viene aperta la pagina di Custom Deployment sulla console di Azure.

Subscription *	<input type="text" value="SE-Subscription"/>
Resource group *	<input type="text" value="abcd22"/> <a href="#">Create new</a>
Instance details	
Region *	<input type="text" value="(Europe) Italy North"/>
Admin Username *	<input type="text" value="abcd22"/>
Admin Password *	<input type="text" value="*****"/>
Forti Gate Count	<input type="text" value="2"/>
Forti Gate Name Prefix *	<input type="text" value="hub"/>
Forti Gate Image Sku	<input type="text" value="fortinet_fg-vm"/>
Forti Gate Image Version	<input type="text" value="latest"/>
Forti Gate Additional Custom Data	<input type="text"/>
Forti Gate Session Sync	<input type="text" value="false"/>
Forti Gate Probe Response	<input type="text" value="true"/>
Instance Type	<input type="text" value="Standard_F2s"/>
External Load Balancer	<input type="text" value="true"/>
Outbound Connectivity	<input type="text" value="external-nat-device-or-elb"/>
Availability Options	<input type="text" value="Availability Zones"/>
Accelerated Networking	<input type="text" value="true"/>
Accelerated Connections	<input type="text" value="false"/>
Accelerated Connections Sku	<input type="text" value="A1"/>

Compilare il form come in figura:  
Se non già presente selezionare la Subscription del proprio account  
Selezionare il proprio Resource Group creato preminentemente  
Inserire la username amministrativa (si consiglia uguale al nome del proprio Resource Group)  
Inserire la password (se si perde non sarà possibile recuperarla, salvarla eventualmente in un file di testo)  
Inserire **hub** come prefisso  
Scorrere e lasciare le altre impostazioni di Default fino a Vnet Name

Vnet Name	<input type="text" value="hub-abcd22"/>
Vnet Resource Group	<input type="text"/>
Vnet Address Prefix	<input type="text" value="172.16.136.0/22"/>
Subnet1Name	<input type="text" value="externalsubnet"/>
Subnet1Prefix	<input type="text" value="172.16.136.0/26"/>
Subnet1Start Address	<input type="text" value="172.16.136.4"/>
Subnet2Name	<input type="text" value="internalsubnet"/>
Subnet2Prefix	<input type="text" value="172.16.136.64/26"/>
Subnet2Start Address	<input type="text" value="172.16.136.68"/>
Subnet3Name	<input type="text" value="protectedsubnet"/>
Subnet3Prefix	<input type="text" value="172.16.138.0/26"/>
Serial Console	<input type="text" value="yes"/>
Forti Manager	<input type="text" value="no"/>

Vnet Name : hub-<resource gorup>  
(per es. hub-abcd22)  
Scorrere e lasciare le impostazioni di default fino a Fortigate License FortiFlex

Forti Gate License BYOL7 ⓘ	<input type="text"/>
Forti Gate License BYOL8 ⓘ	<input type="text"/>
Forti Gate License Forti Flex1 ⓘ	<input checked="" type="text"/> 9BC3828CC6C26F7D989B
Forti Gate License Forti Flex2 ⓘ	<input checked="" type="text"/> CFABD9A7C1C83193393E
Forti Gate License Forti Flex3 ⓘ	<input type="text"/>
Forti Gate License Forti Flex4 ⓘ	<input type="text"/>
Forti Gate License Forti Flex5 ⓘ	<input type="text"/>
Forti Gate License Forti Flex6 ⓘ	<input type="text"/>
Forti Gate License Forti Flex7 ⓘ	<input type="text"/>
Forti Gate License Forti Flex8 ⓘ	<input type="text"/>
Custom Image Reference ⓘ	<input type="text"/>
Location ⓘ	<input type="text"/> [resourceGroup().location]
Tags By Resource	<input type="text"/> {} <span style="color: green;">✓</span>
Fortinet Tags	<input type="text"/> {"publisher":"Fortinet","template":"Active-Active-ELB-ILB","provider":6... <span style="color: green;">✓</span>

[Previous](#) [Next](#) [Review + create](#)

Inserire in FortiFlex1 e FortiFlex2 due dei tre token ricevuti via mail.

Se non ancora ricevuti lasciare i due campi vuoti e proseguire.

Selezionare **NEXT**

Selezionare **Create**

### 3. HUB - Creazione Azure Route Server

In attesa che il deployment termini, tornare all'elenco delle proprie risorse, creare Azure Route Server che gestirà il routing dinamico via BGP tra il cluster Fortigate e il routing della vnet HUB.

Elemento necessario per il route server è la creazione di una nuova subnet /27 con nome RouteServerSubnet all'interno della vnet.

Selezionare in alto al destro su **Microsoft Azure** (sempre presente in qualunque schermata della console) e successivamente selezionare il proprio resource Group

The screenshot shows the Azure portal interface. At the top, there's a blue header bar with the 'Microsoft Azure' logo (circled in red), a search bar ('Search resources, services, and docs (G+/)'), and a user profile icon. Below the header is a 'Azure services' section with various icons and links. The main area is titled 'Resources' with tabs for 'Recent' and 'Favorite'. A table lists resources: one row for 'abcd22' (Resource group) with 'Type' as 'Resource group' and 'Last Viewed' as 'a few seconds ago'. At the bottom, there's a detailed list of resources under 'Recent' with columns for name, type, and status. A dropdown menu for 'Type' is open, showing options like Virtual network, Virtual machine, Route table, etc., with 'Virtual network' currently selected (also circled in red).

Selezionare il nome della colonna Type per mettere in ordine le risorse

Selezionare la vnet hub-xxxxxxx

Nel menu a sinistra selezionare **Settings -> Subnet**

**Notate che nessuna subnet ha associata una tabella di routing.**

In alto selezionare **+Subnet**

## Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose	Route Server
Name *	RouteServerSubnet
IPv4	
Include an IPv4 address space	<input checked="" type="checkbox"/>
IPv4 address range *	172.16.136.0/22 172.16.136.0 - 172.16.139.255
Starting address *	172.16.137.0
Size	/27 (32 addresses)
Subnet address range	172.16.137.0 - 172.16.137.31
IPv6	
Include an IPv6 address space	<input type="checkbox"/> This virtual network has no IPv6 address ranges.
Private subnet <a href="#">[PREVIEW]</a>	
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. <a href="#">Learn more</a>	
Enable private subnet (no default outbound access) <input type="checkbox"/>	
<a href="#">Add</a> <a href="#">Cancel</a> <a href="#">Give feedback</a>	

Inerire le opzioni come in figura a fianco:

Subnet purpose: Route Server

Automaticamente viene impostato il nome della subnet.

IPV4 address range, lasciare la VNET

Starting Address 172.16.137.0

Size: /27

## Selezionare ADD

Ritornare alla **home** della console e selezionare **Marketplace**



Nel campo search digitare **Azure route server** e dare invio

Home >

## Marketplace

Get Started

Service Providers

In Route Server selezionare **Create** e poi **Route Server**

Management

Showing 1 to 20 of 21 results for 'azur'

Private Marketplace

Private Offer Management

## My Marketplace

Favorites

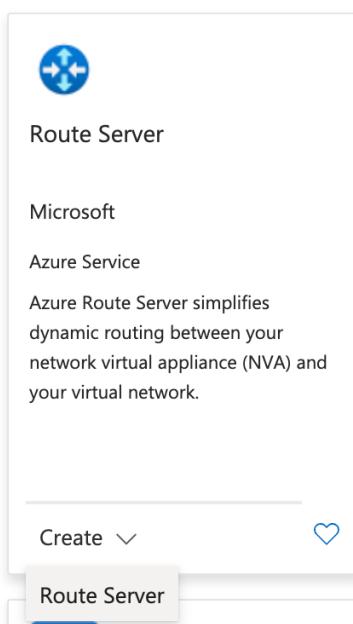
My solutions

Recently created

Private plans

## Categories

Security (15)



**Create a Route Server** ...

Subscription *	SE-Subscription	Compilare i parametri come da figura a fianco.
Resource group *	abcd22 <a href="#">Create new</a>	Usare come nome del router ARS<nome resource group>
Instance details		Routing Preference: ASPath
Name *	ARSabcd22	Vnet hub e subnet creata precedentemente.
Region *	Italy North	
Routing Preference *	<input type="radio"/> ExpressRoute <input type="radio"/> VPN <input checked="" type="radio"/> ASPath	
<p><span style="color: #0078D4;">i</span> Route Server will prefer the connection with the shortest AS Path.</p>		
<b>Configure virtual networks</b>		
Virtual network *	hub-abcd22 <a href="#">Create new</a>	<b>Review + create -&gt; Create</b>
Subnet *	RouteServerSubnet (172.16.137.0/27) <a href="#">Manage subnet configuration</a>	
<b>Public IP address</b>		
Public IP address *	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing	
Public IP address name *	hub-abcd22-ip	
<a href="#">Review + create</a> <a href="#">Previous</a> <a href="#">Next : Tags &gt;</a> <a href="#">Download a template for automation</a>		

Il deployment dell'Azure Route server può impiegare alcuni minuti.

Iniziare a creare nella ProtectedSubnet della vnet HUB una VM Linux che verrà utilizzata per i test.

## 4. HUB - Creazione server Ubuntu01

Tornare nella Home della console Azure e entrare nel Marketplace.

Nel campo search digitare **ubuntu server** e dare invio

Home > Marketplace ... Selezione **Ubuntu Server 22.04 -> Create**

Get Started Service Providers Management Private Marketplace Private Offer Management My Marketplace Favorites My solutions Recently created Private plans Categories Compute (540) Developer Tools (461) Instance details Virtual machine name \* hub-ubuntu-01 Region \* (Europe) Italy North Availability options Availability zone Zone 1 You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more Security type Standard Image \* Ubuntu Server 22.04 LTS - x64 Gen2 See all images | Configure VM generation This image is compatible with additional security features. Click here to swap to the Trusted launch security type. VM architecture Arm64 x64 Run with Azure Spot discount Run with Azure Spot discount Size \* Standard\_B1ms - 1 vcpu, 2 GiB memory (\$17.52/month) Create

Compilare i parametri scorrendo le opzioni fino in fondo

Resource Group : confermare vostro Resource Groupe

VM name: hub-ubuntu-01

Security Type: Standard

Compilare i parametri come da figura

Run with Azure Spot discount

Size \*

Enable Hibernation   
Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more](#)

**Administrator account**

Authentication type  SSH public key  Password

Username \*  ✓

Password \*  ✓

Confirm password \*  ✓

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*  None  Allow selected ports

Select inbound ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

**NEXT**

< Previous Next : Disks > Review + create

**Authentication Type: Password**

**Impostare username = RG name**

**Impostare password**

**No inbound ports**

**NEXT**

## Lasciare le impostazioni di default nella sezione Disk - NEXT

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.  
[Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \*

Subnet \*

Public IP  None

NIC network security group  None  Basic  Advanced

Delete NIC when VM is deleted

Enable accelerated networking  The selected VM size does not support accelerated networking.

**Load balancing**

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options  None  Azure load balancer Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.  Application gateway Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL

### **Networking**

**Compilare i parametri di rete come da figura**

**Selezionare**

**La propria HUB-vnet**

**ProtectedSubnet**

**NIC security Group None**

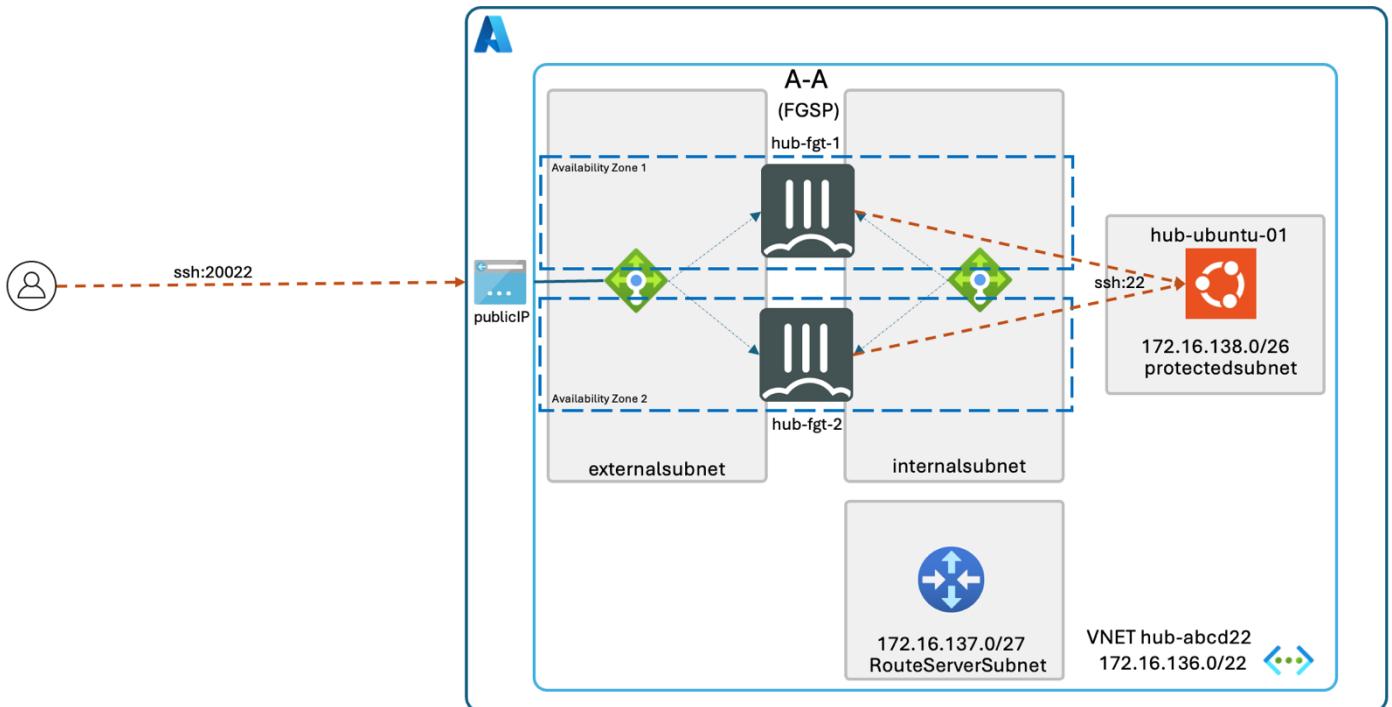
**No Public IP**

**Review + create**

**Create**

< Previous Next : Management > Review + create

## 5. HUB - Accesso server Ubuntu01 tramite VIP cluster



Per abilitare la connessione SSH via internet da client esterno al server Ubuntu occorre completare i seguenti task:

- Creazione regola sul loadbalancer per gestire la porta che verrà utilizzata per veicolare la sessione ssh ( non è possibile in questo caso usare direttamente la porta 22 poichè già usata per gestire i firewall, usare la porta 20022)
- Creazione VIP con port-forwarding sui Fortigate
- Creazione regola sui Fortigate

Dalla home di Azure cliccare il proprio resource group

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, there's a 'Azure services' section with various icons for creating resources and managing them. The main area is titled 'Resources' and shows a list of recent and favorite resources. One resource, 'abcd22', is circled in red.

Type	Last Viewed
Resource group	a few seconds ago
Load balancer	15 minutes ago
Virtual machine	15 hours ago
Virtual machine	15 hours ago
Virtual machine	15 hours ago
Virtual machine	15 hours ago
Network interface	15 hours ago
Route table	15 hours ago
NAT gateway	15 hours ago
Public IP address	15 hours ago
Resource group	15 hours ago

Dall'elenco delle risorse cliccare **hub-externalloadbalancer**

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the text "Microsoft Azure". Below it, the navigation bar shows "Home > abcd22 > hub-externalloadbalancer". The main content area has a title "hub-externalloadbalancer | Load balancing rules" with a star icon and three dots. To the right, the text "Dal menu selezionare **Settings**" is displayed. On the left, there's a sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (which is expanded to show Frontend IP configuration, Backend pools, Health probes, Load balancing rules, Inbound NAT rules, Outbound rules, Properties, Locks, Monitoring, Automation, and Help). The "Load balancing rules" option is selected and highlighted in grey.

Dal menu selezionare **Settings**

## Load balancing rules

### Selezionare **Add**

Name ↑	Protocol ↑
ExternalLBRule-FE-http	TCP/80
ExternalLBRule-FE-udp10551	UDP/10551

## Add load balancing rule

hub-externalloadbalancer

The form for adding a new load balancing rule is shown. It includes fields for Name (tcp\_20022), IP Version (IPv4 selected), Frontend IP address (hub-elb-externalsubnet-frontend (172.213.177.73)), Backend pool (hub-elb-externalsubnet-backend), Protocol (TCP selected), Port (20022), Backend port (20022), Health probe (lbprobe (TCP:8008) selected), Session persistence (None), Idle timeout (minutes) (4), Enable TCP Reset (unchecked), Enable Floating IP (checked), and Outbound source network address translation (SNAT) (checkboxes for "Use default port allocation" and "(Recommended) Use outbound rules" are present, with "Use default port allocation" selected).

Compilare i parametri come in figura a fianco.

L'attivazione del parametro Floating IP disabilita il DNAT sul bilanciatore.

I fortigate vedranno come ip destinatario l'ip pubblico del bilanciatore.

Lo stesso ip verrà configurato nel prossimo step come VIP sul Fortigate.

### Save

**Save**

**Cancel**

Per accedere alla gui dei fortigate occorre utilizzare l'ip pubblico dell' ExternalLoadBalancer (Frontend IP nella figura sotto) e sfruttare le regole di inbound NAT (port forwarding) create automaticamente dal template.

Le regole di inbound NAT sono gestite all'interno della configurazione dell'ExternalLoadBalancer -> Settings -> inbound NAT rules

Home > abcd22 > hub-externalloadbalancer

Name	Frontend IP	Frontend port/range	Target	Service
hub-fgt-2-MGMT-SSH	172.213.197.164	50031	hub-fgt-2	SSH (TCP/22)
hub-fgt-2-MGMT-HTTPS	172.213.197.164	40031	hub-fgt-2	HTTPS (TCP/443)
hub-fgt-1-MGMT-SSH	172.213.197.164	50030	hub-fgt-1	SSH (TCP/22)
hub-fgt-1-MGMT-HTTPS	172.213.197.164	40030	hub-fgt-1	HTTPS (TCP/443)

Gui HTTPS di hub-fg-1: porta 40030

Gui HTTPS di hub-fg-2: porta 40031

SSH hub-fg-1: porta 50030

SSH hub-fg-2: porta 50031

Dopo l'accesso ai Fortigate hub inserire il token FortiFlex se non già configurato al lancio del template.

Accedere alla gui https dei due fortigate ( hub-fg-1 e hub-fg-2 ) e configurare vip con port-forwarding

Creare un oggetto con il proprio ip address pubblico e infine la regola per l'accesso SSH

Name	SSH_ubuntu_01
Type	Standard ZTNA
Incoming interface	port1
Outgoing interface	port2
Source	myip
Security posture tag	+ + + + +
Destination	vip_20022
Schedule	always
Service	SSH tcp_20022
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection mode	Flow-based Proxy-based
Firewall/Network Options	
NAT	<input checked="" type="checkbox"/>
IP pool configuration	<input type="radio"/> Use Outgoing Interface Address <input checked="" type="radio"/> Use Dynamic IP Pool

La regola deve avere il source nat per due motivi: la protected subnet, come notato precedentemente, non ha alcuna routing table associata quindi non saprebbe a chi girare il traffico destinato ad un client fuori VNET

Se anche venisse impostato il default gateway verso il bilanciatore interno, le sessioni avrebbero il 50% di probabilità di andare in out-of state poiché i due bilanciatori non comunicano tra di loro e non effettuano scelte coerenti sulla gestione del traffico: pacchetto in ingress viene girato da external load balancer verso hub-fg-1 e pacchetto in egress viene girato da internal load balancer verso hub-fg-2.

Quest'ultima situazione potrebbe essere risolta tramite FGSP.

In cloud occorre fare però attenzione poiché solo una vCPU si occupa di sincronizzare le sessioni, rischiando di saturarsi in caso di elevato numero di sessioni contemporanee.

Applicare la regola.

## TEST

Accedere in ssh dal proprio client

```
ssh abcd22@x.x.x.x -p 20022
```

Dall'elenco delle sessioni sul fortigate (Dashboard – Fortiview Sessions ) verificare su quale Fortigate il bilanciatore di Azure ha girato la connessione ssh.

Riavviare il gate che sta gestendo la sessione. Attendere una quindicina di secondi (il bilanciatore effettua una probe ogni 5 secondi, alla terza probe fallita considera il nodo down), lanciare una nuova connessione e verificare che la connessione viene correttamente girata sull'altro nodo.

## 6. SPOKE - Creazione Fortigate single-vm

Per il set-up del fortigate del sito spoke utilizzare il wizard direttamente disponibile da marketplace (similmente a quanto fatto precedentemente per il server ubuntu)

Dalla home della console selezionare Marketplace

Home > abcd22 >  
Marketplace ...

Get Started  
Service Providers  
Management  
Private Marketplace  
Private Offer Management  
My Marketplace  
Favorites  
My solutions  
Recently created  
Private plans  
Categories  
Networking (3)  
Security (3)  
AI + Machine Learning (0)  
Analytics (0)  
Dynamically generated content

Showing 1 to 3 of 3 results for 'fortigate byol'. [Clear search](#)

Fortinet FortiGate Next-Generation Firewall  
Fortinet  
Azure Application  
FortiGate NGFW improves on the Azure firewall with complete data, application and network security  
Price varies  
Create ▾ Single VM Active-Passive HA with Fabric Connector Failover Active-Active Loadbalanced with ELB **Single VM** Active-Passive HA with ELB/LB  
Azure Virtual WAN Secured by Fortinet FortiGate  
Fortinet  
Azure Application  
FortiGate NVAs secure North-South, East-West, and internet-bound traffic in Azure vWAN  
Starts at Free  
Create ▾   
Fortinet FortiWeb Web Application Firewall (WAF)  
Fortinet  
Azure Application  
AI-based, multi-layered protection for web-based applications  
Price varies  
Create ▾

Basics Instance Networking Public IP Advanced Review + create

Nel campo search digitare **Fortigate BYOL**

In Fortinet Fortigate Next-Generation Firewall, selezionare

**Create -> Single VM**

Project details  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* SE-Subscription  
Resource group \* abcd22 [Create new](#)

Instance details  
Region \* Italy North

FortiGate Deployment Type - Single VM

FortiGate administrative username \* abcd22

FortiGate password \*

Confirm password \*

Fortigate Name Prefix \* spoke

Fortigate Image SKU Bring Your Own License

Fortigate Image Version latest

FortiGate License  
Bring Your Own License was selected in the basics blade. The license file(s) retrieved from support.fortinet.com can be uploaded here or uploaded after deployment.

My organisation is using the FortiFlex subscription service.

FortiGate FortiFlex C72281029A62659A7B78

Migration between BYOL and PAYG is possible using a redeployment of the VM.

Virtual Machine Name  
Name of the FortiGate VM spoke-FGT

Previous Next Review + create

Compilare i parametri come da figura a fianco.

**Next**

Selezionare Fortiflex e inserire terzo token

**Next**

## Configure Internal Networking

Create a new or select an existing virtual network with the required subnets.

Virtual network

External Subnet \*   172.16.16.0 - 172.16.16.63 (64 addresses)

Internal subnet \* (New) InternalSubnet"/>  172.16.16.64 - 172.16.16.127 (64 addresses)

Protected subnet \* (New) ProtectedSubnet"/>  172.16.17.0 - 172.16.17.255 (256 addresses)

Home &gt; abcd22 &gt; Marketplace &gt; Create Single VM &gt;

spoke-VNET ...

Name \*

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

172.16.16.0/22

This address prefix overlaps with virtual network 'AZG-VNET'. If you intend to peer these virtual networks, change the address space. [Learn more](#)

<input type="text" value="172.16.16.0"/>	<input type="text" value="/22"/>
172.16.16.0 - 172.16.19.255	1,024 addresses

Subnets	IP address range	Size	NAT gateway
ExternalSubnet	172.16.16.0 - 172.16.16.63	/26 (64 addresses)	-
InternalSubnet	172.16.16.64 - 172.16.16.127	/26 (64 addresses)	-
ProtectedSubnet	172.16.17.0 - 172.16.17.255	/24 (256 addresses)	-

## NEXT

The public IP will be used for public services hosted on the FortiGate such as IPSEC termination, management of the FortiGate from external or services behind the Fortigate such as a webserver.

Public IP address

This deployment can use standard or basic SKU public IPs. Moving to a Active/Passive or Active/Active setup requires the use of a standard SKU public IP. Microsoft Azure offers a migration path from a basic to standard SKU public IP.

Il template crea automaticamente una VNET con 3 subnet.

**Edit virtual network** per modificare il nome della vnetNel campo nome inserire **spoke-<nome resource group>****SAVE**Selezionare **Create new** per modificare le opzioni del Public IP associato al FortigateCreate public IP address 

Impostare i parametri come in figura

Name \*

 SKU \*  Basic  StandardRouting preference  Microsoft network  Internetin basso a destra selezionare **OK**

## Review + create

## Create

The screenshot shows the Azure portal interface for a deployment named 'fortinet.fortinet-fortigate-20240724080' in a resource group 'abcd22'. The deployment status is 'Deployment succeeded'. A red circle highlights the 'Notifications' icon in the top navigation bar. Below the notifications, there is a link to 'More events in the activity log'.

Attendere qualche minuto per permettere al deployment di terminare la creazione di tutti le risorse.

In alto a destra potete accedere alle notifiche per verificare lo stato dei task

Deployment succeeded  
Deployment 'fortinet.fortinet-fortigate-20240724080' group 'abcd22' was successful.

Pin to dashboard Go to resource group

Per accedere al fortigate utilizzare direttamente l'ip pubblico che Azure ha associato alla nic esterna.

Dall'elenco delle risorse nel proprio Resource Group selezionare la virtual machine spoke-FGT

The screenshot shows the Azure portal details for a virtual machine named 'spoke-FGT'. The 'Overview' tab is selected. The 'Essentials' section displays the following information:

Essentials	
Resource group	(move) : abcd22
Status	: Running
Location	: Italy North
Subscription	(move) : SE-Subscription
Subscription ID	: cf72478e-c3b0-4072-8f60-41d037c1d9e9
Tags	: provider:6EB3B02F-50E5-4A3E-8CB8-2E12925831VM

On the right side, detailed VM properties are listed:

Operating system	: Linux (FortiOS v7.4.4)
Size	: Standard F2s (2 vcpus, 4 GiB memory)
Public IP address	: 4.232.144.110
Virtual network/subnet	: spoke-fgt-vmf62g.italynorth.cloudapp.azure.com
DNS name	: spoke-fgt-rtpaotsmf62g.italynorth.cloudapp.azure.com
Health state	: -
Time created	: 7/19/2024, 9:39 AM UTC

Se non già inserito durante il wizard accedere alla gui https del fortigate e attivare la licenza mediante il token fortiflex (utilizzare il terzo token ricevuto via mail).

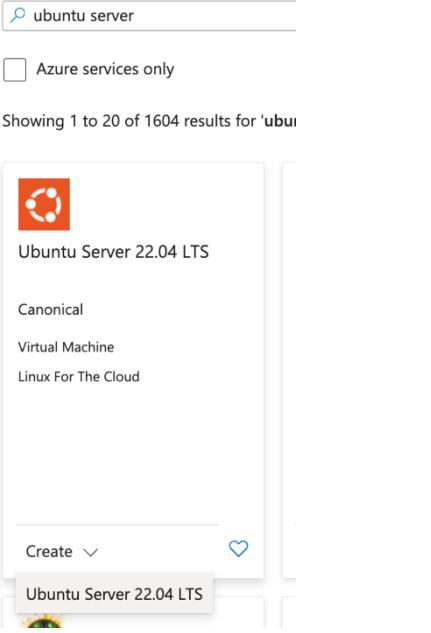
## 7. SPOKE - Creazione server Ubuntu03

Tornare nella Home della console e entrare nel Marketplace.

Nel campo search digitare **ubuntu server** e dare invio

Home > Resource groups > abcd22 > Marketplace

Selezionare **Ubuntu Server 22.04 -> Create**



Get Started

Service Providers

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Compute (540)

Developer Tools (461)

Subscription \* ⓘ

Resource group \* ⓘ

Virtual machine name \* ⓘ

Region \* ⓘ

Availability options ⓘ

Availability zone \* ⓘ

Security type ⓘ

Image \* ⓘ

Compilare i parametri scorrendo le opzioni fino in fondo

Run with Azure Spot discount

Size \*

Enable Hibernation   
Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more](#)

**Administrator account**

Authentication type  SSH public key  Password

Username \*  ✓

Password \*  ✓

Confirm password \*  ✓

**Inbound port rules**  
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*  None  Allow selected ports

Select inbound ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

**Impostare password**

**No inbound ports**

**NEXT**

[< Previous](#) [Next : Disks >](#) **Review + create**

## Lasciare le impostazioni di default nella sezione Disk - **NEXT**

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \*

Subnet \*

Public IP  None  Create new

NIC network security group  None  Basic  Advanced

Delete NIC when VM is deleted

Enable accelerated networking   
The selected VM size does not support accelerated networking.

**Networking**

**Compilare i parametri di rete come da figura**

**Selezionare**

**La vnet *spoke-<name>***

**ProtectedSubnet**

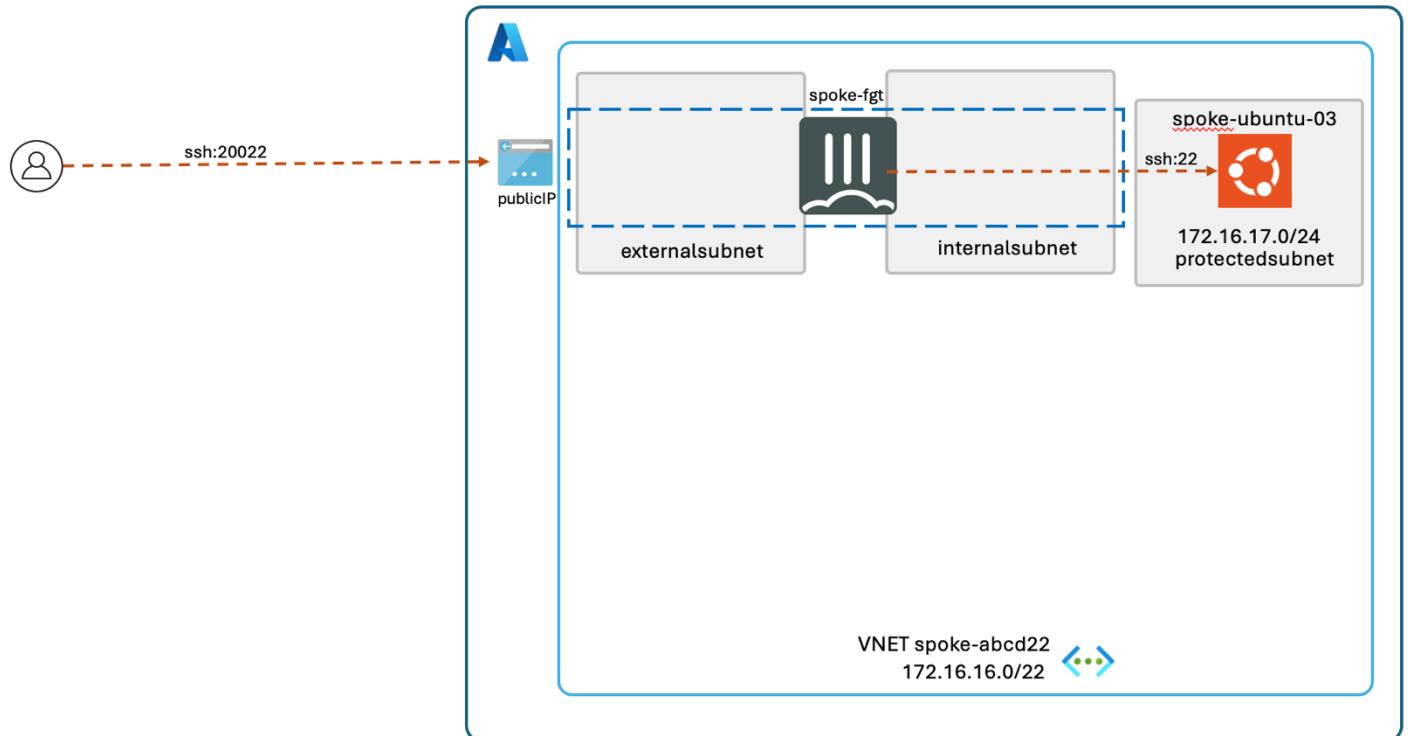
**No Public IP**

**Review + create**

**Create**

[< Previous](#) [Next : Management >](#) **Review + create**

## 8. SPOKE - Accesso server Ubuntu03 tramite VIP Fortigate spoke



Per accedere al server Ubuntu03 sfruttiamo il Public ip associato alla interfaccia esterna del gate.

La subnet ProtectedSubnet ha associata una routing table che imposta il default gateway verso l’interfaccia internet del fortigate,

Home > abcd22 > spoke-VNET

**spoke-VNET | Subnets**

Virtual network

Search		Subnet	Gateway subnet	Refresh	Manage users	Delete
		ExternalSubnet	172.16.16.0/26	-	58	-
		InternalSubnet	172.16.16.64/26	-	58	-
		ProtectedSubnet	172.16.17.0/24	-	250	-

**Route table**

spoke-RouteTable-ProtectedSubnet

Home > abcd22 > spoke-VNET | Subnets >

**spoke-RouteTable-ProtectedSubnet**

Route table

Search		Move	Delete	Refresh	Give feedback
<b>Overview</b>		Resource group (move) : abcd22 Location : Italy North Subscription (move) : SE-Subscription Subscription ID : cf72478e-c3b0-4072-8f60-41d037c1d9e9 Tags (edit) : provider : 6EB3B02F-50E5-4A3E-8CB8-2E12925831VM			
<b>Associations</b>		1 subnet associations			
<b>Routes</b>		Routes Search routes			
		Name	Address prefix	Next hop type	Next hop IP address
		Default	0.0.0.0/0	Virtual appliance	172.16.16.68
		Subnet	172.16.17.0/24	Virtual network	-
		VirtualNetwork	172.16.16.0/22	Virtual appliance	172.16.16.68
<b>Subnets</b>		Subnets Search subnets			
		Name	Address range	Virtual network	Security group
		ProtectedSubnet	172.16.17.0/24	spoke-VNET	-

Non occorrerà quindi attivare il NAT nella policy per il flusso in ingresso.

Poiché viene riutilizzato lo stesso ip pubblico del fortigate (utilizzato anche per la gestione amministrativa) occorre configurare il vip con portforwarding, selezionare per esempio ancora la porta 20022.

The screenshot shows the configuration of a static NAT rule. The 'Name' field is set to 'vip\_spoke'. The 'Interface' is 'port1', 'Type' is 'Static NAT', 'External IP address/range' is '0.0.0.0', 'Map to' is '172.16.17.4', and 'Protocol' is 'TCP'. Under 'Port Mapping Type', 'One to one' is selected. The 'External service port' is '20022' and the 'Map to IPv4 port' is '22'. At the bottom are 'OK' and 'Cancel' buttons.

Accedere a spoke-FGT e iniziare a creare il vip.

Lasciare come External IP 0.0.0.0 poichè il network di Azure effettua il DNAT del public ip con l'ip privato della external subnet. (In questo caso non viene mantenuto il Public IP come con l'opzione Floating IP su ExternalLoadBalancer visto precedentemente).

The screenshot shows the creation of a new policy. The 'Name' is 'SSH\_spoke\_ubuntu', 'Type' is 'Standard ZTNA', 'Incoming interface' is 'port1', 'Outgoing interface' is 'port2', 'Source' is 'myip', 'Destination' is 'vip\_spoke', 'Schedule' is 'always', 'Service' includes 'tcp\_20022' and 'SSH', 'Action' is 'ACCEPT', and 'Inspection mode' is 'Flow-based'. Below are sections for 'Firewall/Network Options' (NAT is off) and 'Security Profiles'. At the bottom are 'OK' and 'Cancel' buttons.

Creare come fatto sul cluster il servizio tcp\_20022 e l'oggetto MyIP e infine la policy.

Accedere al server spoke-ubuntu-03 utilizzando l'ip pubblico associato a spoke-FGT

```
ssh abcd22@y.y.y.y -p20022
```

## 9. Configurazione BGP all'interno della vnet HUB

All'inizio del laboratorio è stato creato L'Azure Route Server. Procedere ora alla configurazione del BGP.

The screenshot shows the Azure portal interface for the 'abcd22' resource group. On the left, there's a sidebar with various navigation options like Home, Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The 'Overview' tab is selected. In the main content area, under the 'Essentials' section, it shows the Subscription (move) to 'SE-Subscription', Subscription ID 'cf72478e-c3b0-4072-8f60-41d037c1d9e9', and Tags (edit) with 'CreatedOnDate' set to '2024-07-10T'. Below this is a 'Resources' section with a 'Recommendations (3)' tab. A search bar and filter options ('Type equals all') are present. It lists several resources: 'hub-abcd22-ip', 'hub-externalloadbalancer-pip', 'spoke-FGT-PIP', 'ARSabcd22' (which is highlighted with a red box), 'hub-routetable', 'spoke-RouteTable-ProtectedSubnet', and 'hub-fgt-1'. A note on the right side says: 'Dalla lista delle risorse all'interno del proprio Resource Group click su ARS<resource group name>'.

The screenshot shows the 'ARSabcd22' Route Server settings page. The left sidebar includes Overview, Activity log, Access control (IAM), Tags, Settings (expanded), Configuration, and Peers. The 'Peers' tab is selected. The 'Essentials' section displays the Resource group 'abcd22', Location 'italynorth', Subscription 'SE-Subscription', Subscription ID 'cf72478e-c3b0-4072-8f60-41d037c1d9e9', and Tags (edit). On the right, it shows Provisioning State 'Succeeded', Connectivity Status 'Succeeded', Virtual Network / Subnet 'ARSabcd22', ASN '65515', and Peer Ips '172.16.137.5, 172.16.137.4'. A red box highlights the 'Peer Ips' field.

( L'ASN e i due ip del ASR verranno utilizzati più avanti per configurare i neighbor sui fortigate hub )

The screenshot shows the 'Peers' section of the 'ARSabcd22' Route Server. The left sidebar has the 'Peers' tab selected. At the top, there's a search bar, an 'Add' button, and a 'Refresh' button. Below is a table with a single row for 'Name' and 'No results'. The bottom of the sidebar shows other tabs: Overview, Activity log, Access control (IAM), Tags, Settings, Configuration, Peers (selected), and Properties.

Nel menu a sinistra del Route Server selezionare

**Settings -> Peers**

Nel menu in alto selezionare **ADD**

<b>Add Peer</b>	×	<b>Add Peer</b>  Name * <input type="text" value="hub-fgt-2"/> ✓ ASN * ⓘ <input type="text" value="65400"/> ✓ IPv4 Address * <input type="text" value="172.16.136.70"/> ✓	×	Inserire i due fortigate hub come due nuovi peer:  nome peer ASN 65400 ip address della rispettiva interfaccia interna SAVE
-----------------	---	---	---	--

Attenzione: attendere che Azure finisca di creare il primo peer e poi aggiungere il secondo.

Entrare sulla CLI dei due fortigate hub per completare la configurazione BGP:

Local AS : 65400

Come Router ID inserire il corrispettivo ip della nic interna (port2)

Aggiungere i due ip dell'ASR individuati precedentemente e impostare l'opzione **Enforce eBGP multihop** per permettere il ruolo di route server al servizio ARS.

hub-fgt-1	hub-fgt-2
<pre> config router bgp   set as 65400   set router-id 172.16.136.69   set keepalive-timer 2   set holdtime-timer 8   config neighbor     edit 172.16.137.4       set ebgp-enforce-multihop enable       set remote-as 65515     next     edit 172.16.137.5       set ebgp-enforce-multihop enable       set remote-as 65515     next   end end </pre>	<pre> config router bgp   set as 65400   set router-id 172.16.136.70   set keepalive-timer 2   set holdtime-timer 8   config neighbor     edit 172.16.137.4       set ebgp-enforce-multihop enable       set remote-as 65515     next     edit 172.16.137.5       set ebgp-enforce-multihop enable       set remote-as 65515     next   end end </pre>

## TEST

Da cli verificare il routing

```

get router info bgp summary
get router info bgp network
get router info routing-table all

```

I fortigate hub ricevono la network 172.16.136.0/22 tramite bgp ma non la usano poiché c'è una rotta statica configurata (rotte statiche hanno distanza preferenziale)

Controllare le rotte statiche configurate automaticamente tramite template sempre sui fortigate hub

Destination	Gateway IP	Interface	Status
0.0.0.0/0	172.16.136.1	port1	Enabled
172.16.136.0/22	172.16.136.65	port2	Enabled
168.63.129.16/32	172.16.136.1	port1	Enabled
168.63.129.16/32	172.16.136.65	port2	Enabled

E' possibile modificare la statica per la 172.16.136.0/22 e sostituirla con la 172.16.137.0/27 per indirizzare ricorsivamente tutta la network della vnet

Edit Static Route

Destination Subnet Internet Service  
172.16.137.0/255.255.255.224

Gateway Address  
172.16.136.65

Interface  
port2 x  
+ x

Administrative Distance 10

Comments  
Write a comment... 0/255

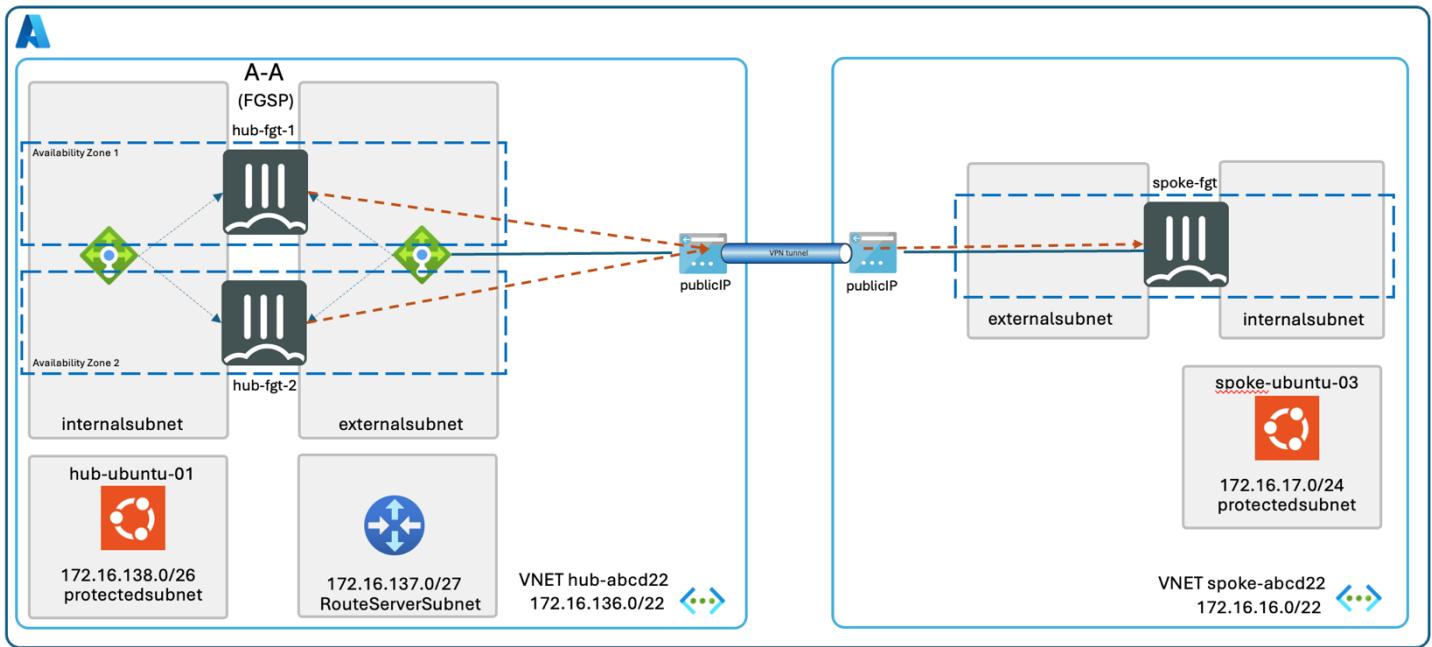
Status Enabled Disabled

Advanced Options

Da CLI verificare la ricorsività della network 172.16.136.0/22

```
get router info routing-table all
```

## 10. Configurazione VPN tra HUB e SPOKE



L'esercizio si compone di 10 step:

- 1 creazione regole di load balancing su Azure per gestire ike e nat traversal
- 2 configurazione ipsec sui fortigate **hub**
- 3 configurazione interfaccia ipsec sui fortigate **hub**
- 4 configurazione bgp su fortigate **hub**
- 5 configurazione secondary ip address sui fortigate **hub**
- 6 creazione regola sui fortigate **hub**
- 7 configurazione ipsec su fortigate **spoke**
- 8 configurazione interfaccia ipsec su fortigate **spoke**
- 9 configurazione bgp su fortigate **spoke**
- 10 creazione regola su fortigate **spoke**

per le interfacce IPSEC verranno usati gli ip 10.10.1.1 per i nodi hub e 10.10.1.2 per il nodo spoke.

### 10.1. creazione regole di load balancing

L'HUB riceverà i tunnel tramite bilanciatore, iniziare a configurare le regole di balancing su **hub-externalloadbalancer** per permettere la gestione di UDP 500 (ike) e UDP 4500 (ipsec nat traversal). Dall'elenco delle risorse nel proprio Resource Group selezionare **hub-externalloadbalancer**. Dal menu a destra selezionare **Settings -> Load Balancing Rules**

Selezionare **ADD** nel menu in alto e inserire due regole, una per udp 500 e una per udp 4500.

Name *	udp_500	Name *	udp_4500
IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Frontend IP address * ⓘ	hub-elb-externalsubnet-frontend (172.213.177.73)	Frontend IP address * ⓘ	hub-elb-externalsubnet-frontend (172.213.177.73)
Backend pool * ⓘ	hub-elb-externalsubnet-backend	Backend pool * ⓘ	hub-elb-externalsubnet-backend
Protocol	<input type="radio"/> TCP <input checked="" type="radio"/> UDP	Protocol	<input type="radio"/> TCP <input checked="" type="radio"/> UDP
Port *	500	Port *	4500
Backend port * ⓘ	500	Backend port * ⓘ	4500
Health probe * ⓘ	Ibprobe (TCP:8008) Create new	Health probe * ⓘ	Ibprobe (TCP:8008) Create new
Session persistence ⓘ	Client IP	Session persistence ⓘ	Client IP
Enable Floating IP ⓘ	<input checked="" type="checkbox"/>	Enable Floating IP ⓘ	<input checked="" type="checkbox"/>
Outbound source network address translation (SNAT) ⓘ	<input type="radio"/> (Recommended) Use outbound rules to provide backend pool members access to the internet. <a href="#">Learn more.</a> ⓘ <input checked="" type="radio"/> Use default port allocation to provide backend pool members with a minimal set of SNAT ports. This is not recommended because it can cause SNAT port exhaustion. <a href="#">Learn more.</a> ⓘ	Outbound source network address translation (SNAT) ⓘ	<input type="radio"/> (Recommended) Use outbound rules to provide backend pool members access to the internet. <a href="#">Learn more.</a> ⓘ <input checked="" type="radio"/> Use default port allocation to provide backend pool members with a minimal set of SNAT ports. This is not recommended because it can cause SNAT port exhaustion. <a href="#">Learn more.</a> ⓘ

In **Session persistence** selezionare **Client IP**, in modo che sia la sessione IKE sia la sessione IPSEC incapsulato vengano gestiti dallo stesso nodo.

Abilitare Floating IP affinché i nodi hub vedano lo stesso ip su cui terminare la vpn

**SAVE**

## 10.2. configurazione ipsec sui fortigate hub

```
config vpn ipsec phase1-interface
  edit hub
    set type dynamic
    set interface port1
    set ike-version 2
    set local-gw x.x.x.x (Ip pubblico dell'Externalloadbalancer)
    set peertype any
    set net-device disable
    set exchange-interface-ip enable
    set add-route disable
    set fgsp-sync enable
    set psksecret fortinet
    set dpd-retrycount 8
    set dpd-retryinterval 2
  next
end

config vpn ipsec phase2-interface
  edit hub
    set phase1name hub
  next
end
```

## 10.3. configurazione interfaccia ipsec sui fortigate hub

```
config system interface
  edit hub
    set vdom root
    set ip 10.10.1.1 255.255.255.255
    set type tunnel
    set remote-ip 10.10.1.2 255.255.255.0
    set interface port1
  next
end
```

## 10.4. configurazione bgp sui fortigate hub

```
config router bgp
    config neighbor
        edit 10.10.1.2
            set next-hop-self enable
            set remote-as 65400
        next
    end
end
```

Occorre abilitare il parametro **Next hop self** per permettere ai fortigate hub di propagare verso lo spoke la network della vnet 172.16.136.0/22 utilizzando come next hop l'ip della propria tunnel-interface 10.10.1.1.

## 10.5. configurazione secondary ip address sui fortigate hub

```
config system interface
    edit port1
        set secondary-IP enable
        config secondaryip
            edit 1
                set ip x.x.x.x (Ip pubblico dell'Externalloadbalancer)
            next
        end
    next
end
```

## 10.6. creazione regola sui fortigate hub

```
config firewall policy
    edit 10
        set name vpn-in
        set srcintf hub
        set dstintf port2
        set action accept
        set srcaddr all
        set dstaddr all
        set service ALL
        set schedule always
        set logtraffic all
        set logtraffic-start enable
    next
end
```

## 10.7. configurazione ipsec su fortigate spoke

```
config vpn ipsec phase1-interface
    edit spoke
        set interface port1
        set ike-version 2
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set remote-gw x.x.x.x (Ip pubblico dell'Externalloadbalancer)
        set psksecret fortinet
        set dpd-retrycount 8
        set dpd-retryinterval 2
    next
end
config vpn ipsec phase2-interface
    edit spoke
        set phase1name spoke
        set auto-negotiate enable
    next
end
```

Il bilanciatore impiega dai 10 ai 15 secondi per accorgersi di un fail di un nodo e per girare il traffico vpn su un nuovo nodo attivo. Impostare il DPD con un tempo di identificazione del tunnel down di circa 16 secondi.

## 10.8. configurazione interfaccia ipsec su fortigate spoke

```
config system interface
  edit spoke
    set vdom root
    set ip 10.10.1.2 255.255.255.255
    set type tunnel
    set remote-ip 10.10.1.1 255.255.255.0
    set interface port1
  next
end
```

## 10.9. configurazione bgp su fortigate spoke

```
config router bgp
  set as 65400
  set router-id 172.16.16.68
  set keepalive-timer 1
  set holdtime-timer 9
  config neighbor
    edit 10.10.1.1
      set remote-as 65400
    next
  end
  config network
    edit 1
      set prefix 172.16.16.0 255.255.252.0
    next
  end
end
```

## 10.10. creazione regola su fortigate spoke

```
config firewall policy
  edit 10
    set name spoke-out
    set srcintf port2
    set dstintf spoke
    set action accept
    set srcaddr all
    set dstaddr all
    set service ALL
    set schedule always
    set logtraffic all
    set logtraffic-start enable
  next
end
```

## TEST

Accedere al server spoke-Ubuntu-03

```
ssh abcd22@y.y.y.y -p20022
```

e lanciare ping verso hub-Ubuntu-01 (ping 172.16.138.4)

la vpn viene stabilita su uno dei due fortigate HUB.

Per verificare tabella di routing propagata internamente verso Azure dai Fortigate HUB esistono due modi:

1. Azure Cloud Shell (attivabile da menu in alto a destra)



```
Get-AzRouteServerPeerLearnedRoute –ResourceGroupName abcd22 –RouteServerName ARSabcd22 –PeerName hub-fgt-1
```

```
Get-AzRouteServerPeerLearnedRoute -ResourceGroupName abcd22 -RouteServerName ARSabcd22 -PeerName hub-fgt-2
```

Solo uno dei due comandi mostrerà il nodo che sta propagando la network dello spoke

## 2. console web Azure.

In Azure le rotte vengono applicate direttamente alle nic delle vm

Dall'elenco risorse selezionare **hub-ubuntu-01 -> Networking -> Network Settings**

Home > abcd22 > hub-ubuntu-01

**hub-ubuntu-01 | Network settings** Virtual machine

Search This is a new experience. Please provide feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Connect Networking Network settings Load balancing Application security groups Network manager

Attach network interface Detach network interface View topology

Network interface / IP configuration hub-ubuntu-01502\_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface	:	hub-ubuntu-01502_z1
Virtual network / subnet	:	hub-abcd22 / protectedsubnet
Public IP address	:	- (Configure)
Private IP address	:	172.16.138.4
Admin security rules	:	0 (Configure)

Selezionare la **Network Interface**

Home > abcd22 > hub-ubuntu-01 | Network settings > hub-ubuntu-01502\_z1

**hub-ubuntu-01502\_z1 | Effective routes** Network interface

Search Download Refresh Give feedback

Showing only top 200 records; click Download above to see all.

Overview Activity log Access control (IAM) Tags Settings Monitoring Automation Help Effective security rules Effective routes Support + Troubleshooting

Scope Network interface (hub)

Associated route table: -

Effective routes

Source	↑↓	State	↑↓	Address Prefixes	↑↓	Next Hop Type	↑↓	Next Hop IP Address
Default	Active			172.16.136.0/22		Virtual network		-
Virtual netwo...	Active			172.16.16.0/22		Virtual network gateway		172.16.136.69
Default	Active			0.0.0.0/0		Internet		-
Default	Active			10.0.0.0/8		None		-
Default	Active			127.0.0.0/8		None		-

Dal menu a sinistra **Help-> effective routes**

Dall'elenco individuare la vnet spoke e l'ip del nexthop (interfaccia interna del hub-fgt che sta gestendo la vpn, ossia 172.16.136.69 oppure 172.16.136.70

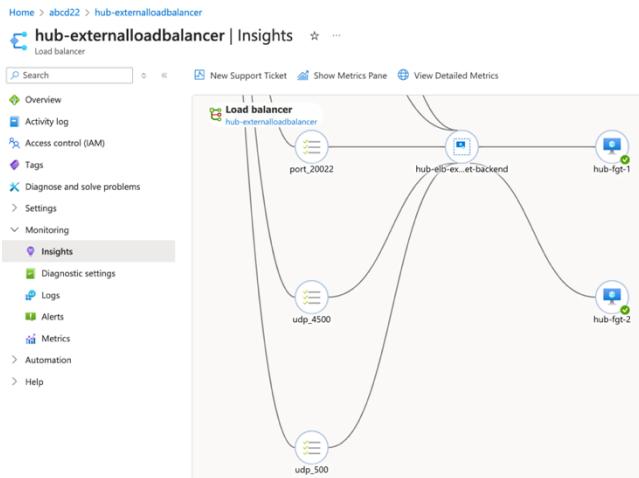
## TEST

Verificare i tempi di failover (un minuto circa) dovuti prevalentemente alle latenze di convergenza del BGP

Spegnere il nodo che sta gestendo la VPN:

il bilanciatore si accorge del fail tra 10 e i 15 secondi (devono fallire 3 probes intervallate da 5 secondi)

Per verificare lo stato del cluster selezionare **hub-externalloadbalancer**



dal menu a sinistra Selezionare **Monitor -> Insights**

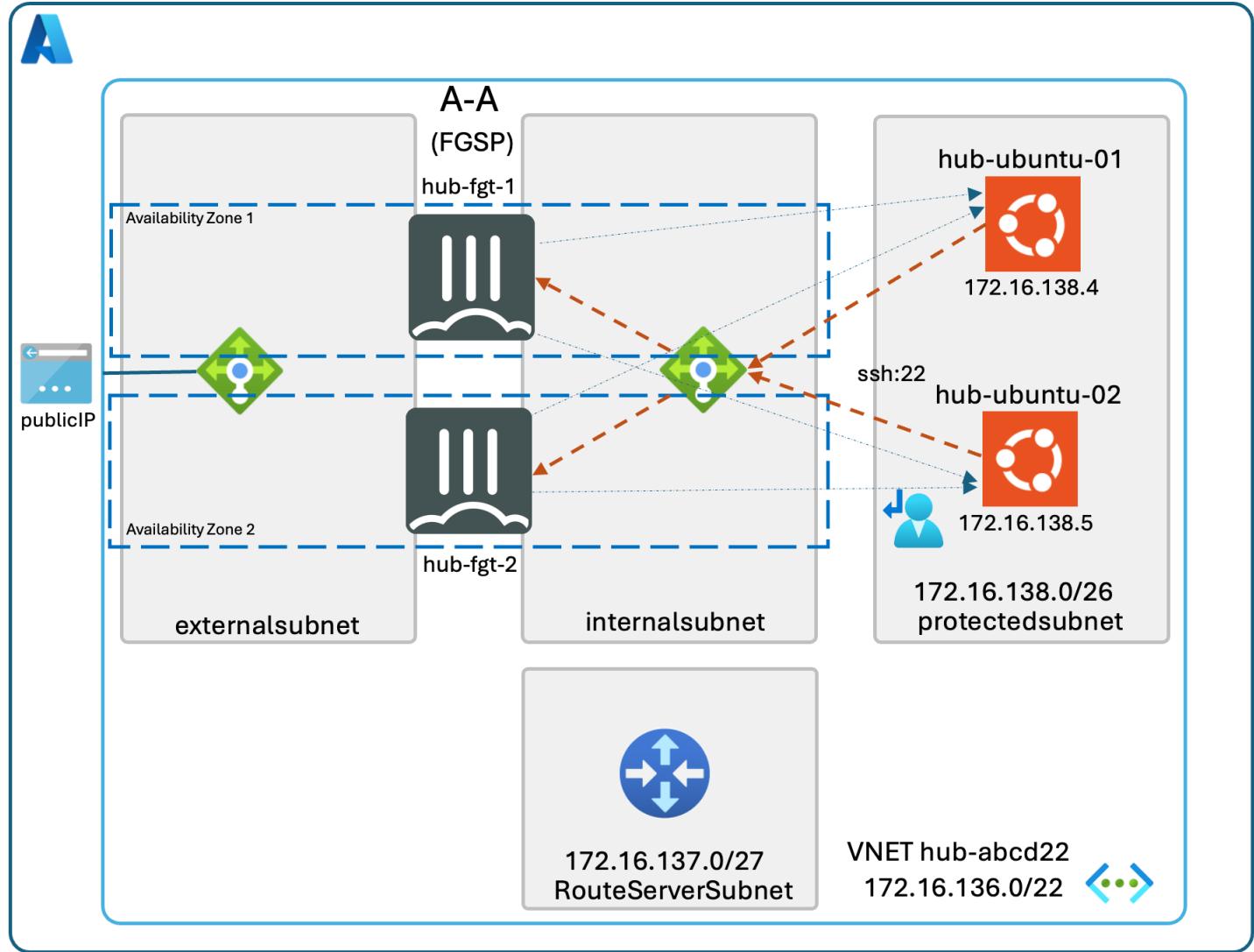
Fare zoom sulle icone dei due nodi fortigate.

Riaccendere il nodo fortigate hub precedentemente spento.

La vpn dopo circa un minuto si risposta sul nodo che è stato riaccesso, perché ?

Il bilanciatore è stato configurato con l'opzione di persistenza su client IP per permettere che sia l'IKE sia il nat-traversal vengano girati sullo stesso nodo. Questo però fa sì che per ogni ip sorgente l'algoritmo del bilanciatore scelga sempre lo stesso nodo target.

## 11. HUB - Microsegmentazione



Verificare come applicare la network security tra due server installati nella stessa subnet.

Una delle caratteristiche di Azure è la possibilità di configurare lo User Defined Routing in modo che possa avere la priorità sulla subnet stessa in cui viene applicata.

Task dell'esercizio:

- installazione del server hub-ubuntu-02 nella Protected Subnet
- configuraione nuova routing table da associare alla Protected Subnet
- configuraione policy sui due nodi hub-fgt per permettere l'SSH
- test flussi

### Installazione di un nuovo server hub-ubuntu-02

Tornare nella Home della console Azure e entrare nel Marketplace.

Nel campo search digitare **ubuntu server** e dare invio

Home > Marketplace ...

Selezionare **Ubuntu Server 22.04 -> Create**

Get Started

Service Providers

Azure services only

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Compute (540)

Developer Tools (461)

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  [Create new](#)

Instance details

Virtual machine name \*

Region \*

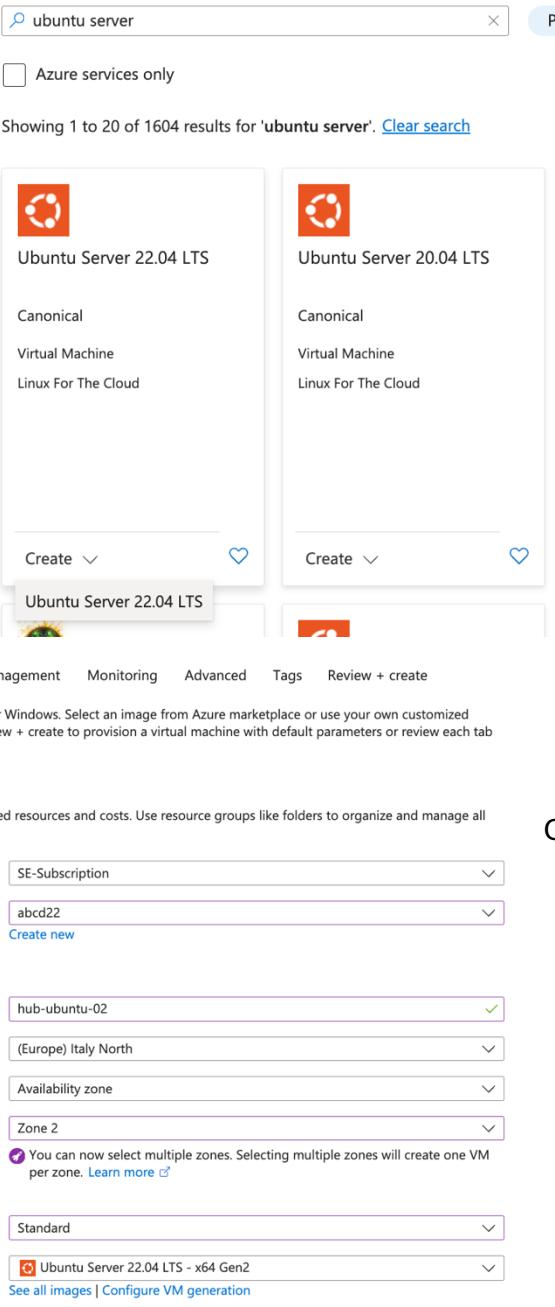
Availability options

Availability zone \*   
You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type

Image \*  [See all images](#) | [Configure VM generation](#)

Compilare i parametri come da figura



Run with Azure Spot discount

Size \*  Standard\_B1ms - 1 vcpu, 2 GiB memory (\$17.52/month)  See all sizes

Enable Hibernation   
i Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more](#)

**Administrator account**

Authentication type  SSH public key  Password

Username \*  ✓

Password \*  ✓

Confirm password \*  ✓

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \*  None  Allow selected ports

Select inbound ports

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

**Impostare password**

**No inbound ports**

**NEXT**

[< Previous](#) [Next : Disks >](#) [Review + create](#)

## Lasciare le impostazioni di default nella sezione Disk - NEXT

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \*  hub-abcd22

Subnet \*  protectedsubnet (172.16.138.0/26)

Public IP  None

NIC network security group  None  Basic  Advanced

Delete NIC when VM is deleted

Enable accelerated networking  The selected VM size does not support accelerated networking.

**Load balancing**

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options  None  Azure load balancer Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.  Application gateway Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL

[< Previous](#) [Next : Management >](#) [Review + create](#)

Al termine del deploy di hub-ubuntu-02 verificarne la raggiungibilità:

**Impostare password**

**No inbound ports**

**NEXT**

## Networking

Compilare i parametri di rete come da figura

Selezionare

La propria HUB-vnet

ProtectedSubnet

No Public IP

**Review + create**

**Create**

accedere in ssh a hub-ubuntu-01 e da qui effettuare ping e accedere in ssh a hub-ubuntu-02

```
ssh abcd22@x.x.x.x -p 20022
```

```
ping 172.16.138.5
```

```
abcd22@hub-ubuntu-01:~$ ssh abcd22@172.16.138.5
```

## Creazione e configurazione nuova routing table

Dalla Home della console entrare nel Marketplace e digitare nel search **route table**

Home > abcd22 > Marketplace ...

Get Started

Service Providers

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Networking (3)

Security (2)

route table

Azure services only

Showng 1 to 5 of 5 results for 'route table'

Route table

Microsoft

Azure Service

Use route tables to control how traffic is directed in a virtual network.

Create Route table

Home > abcd22 > Marketplace >

### Create Route table ...

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ SE-Subscription

Resource group \* ⓘ abcd22

Create new

Instance details

Region \* ⓘ Italy North

Name \* ⓘ hub-routetable-protectedsubnet

Propagate gateway routes \* ⓘ Yes

Impostare i parametri come in figura

Lasciare abilitata l'opzione Propagate routes

### Review + create

### Create

Tornare alla Home e all'elenco delle risorse, selezionare la routing table appena creata

Route table

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

- Configuration
- Routes
- Subnets**
- Properties
- Locks

> Monitoring

> Automation

> Help

Dal menu a sinistra selezionare **Settings -> Subnet**

Dal menu in alto selezionare **Associate**

### Associate subnet

hub-routetable-protectedsubnet

Virtual network ⓘ

hub-abcd22 (abcd22)

Subnet \* ⓘ

protectedsubnet

Selezionare la propria vnet hub e la protectedsubnet.

**OK**

Il prossimo step prevede l'inserimento della rotta statica per indirizzare la protectedsubnet via indirizzo del load balancer interno. Per Recuperare l'ip del load balancer selezionare dall'elenco risorse **hub-internalloadbalancer**.

Load balancer

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Monitoring

Automation

Help

**See more**

Resource group (move)	: abcd22	Backend pool	: hub-ilb-internalsubnet-backend
Location	: Italy North	Load balancing rule	: lbruleFAll
Subscription (move)	: SE-Subscription	Health probe	: lprobe (Tcp:8008)
Subscription ID	: cf72478e-c3b0-4072-8f60-41d037c1d9e9	NAT rules	: 0 inbound
SKU	: Standard	Tier	
Tags (edit)		Private IP address	: 172.16.136.68

L'ip appare a destra

Tornare al setup della routing table **hub-routetable-protectedsubnet**

Sempre dal menu a sinistra selezionare **Settings->Routes**

Dal menu in alto selezionare **Add**

### Add route

hub-routetable-protectedsubnet

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. [Learn more](#)

Route name \*  ✓

Destination type \*  ✓

Destination IP addresses/CIDR ranges \*  ✓

Next hop type \*  ✓

Next hop address \*  ✓

Inserire i parametri come in figura.

**Add**

Il traffico tra tutte le vm all'interno della protected subnet viene da ora girato al bilanciatore interno e da qui ai fortigate hub.

## TEST

Verificare l'impossibilità della sessione ssh tra hub-ubuntu-01 e hub-ubuntu-02.

Nemmeno il ping risponde

```
ssh abcd22@x.x.x.x -p 20022
abcd22@hub-ubuntu-01:~$ ssh abcd22@172.16.138.5
abcd22@hub-ubuntu-01:~$ ping 172.16.138.5
```

## Creazione policy per traffico EST-OVEST

Per abilitare il traffico SSH tra i due server ubuntu creare la policy sui due fortigate hub

Name <span style="color: #0070C0;">i</span>	microsegmentation
Type	Standard ZTNA
Incoming interface	port2
Outgoing interface	port2
Source	hub-ubuntu-01 + hub-ubuntu-02
Security posture tag <span style="color: #0070C0;">i</span>	
Destination	hub-ubuntu-02 + hub-ubuntu-01
Schedule	always
Service	SSH +
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection mode	Flow-based Proxy-based

hub-ubuntu-01: 172.16.138.4  
hub-ubuntu-02: 172.16.138.5

Non è necessario abilitare il NAT poiché le sessioni est-ovest attraversano solo il bilanciatore interno.

Firewall/Network Options

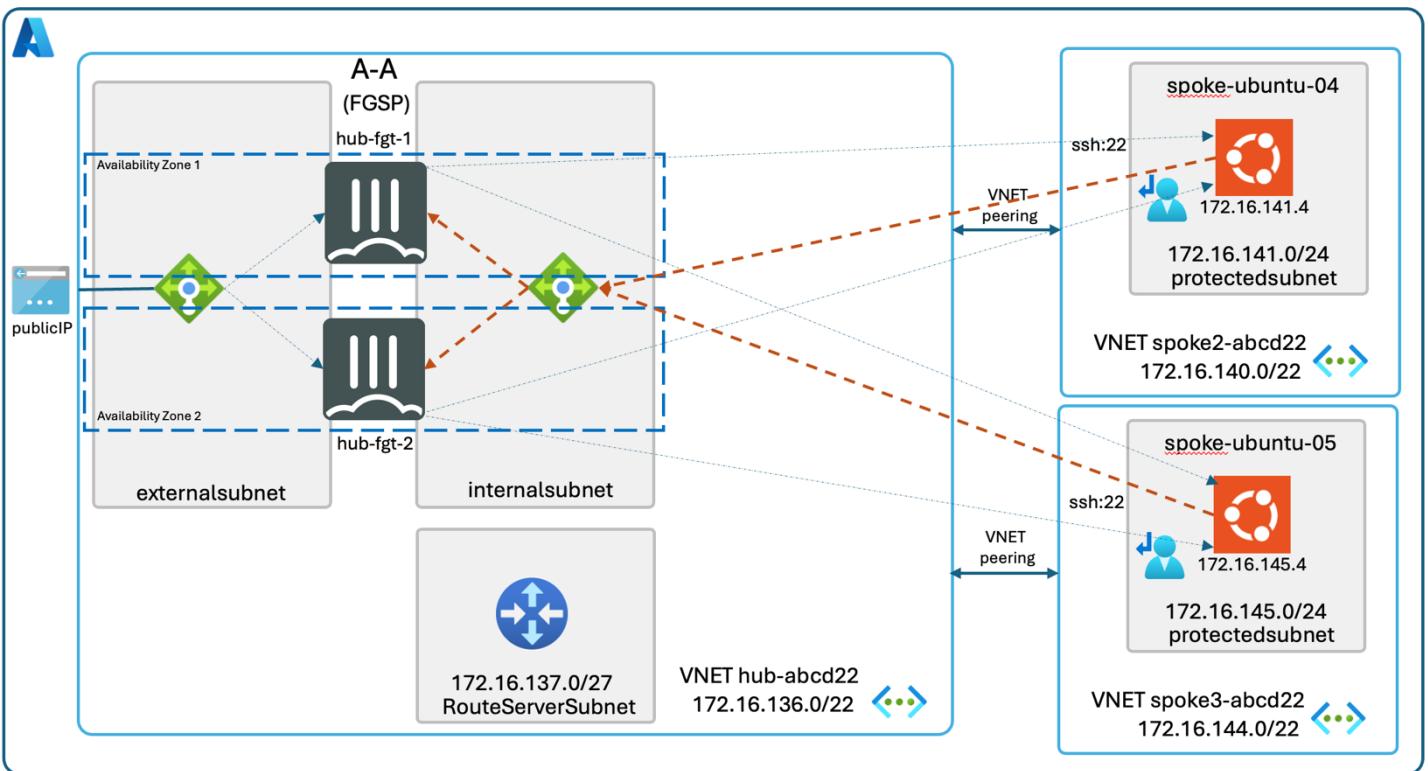
NAT

## TEST

Riprovare ad accedere in ssh da hub-ubuntu-01 a hub-ubuntu-02.

La sessione ssh si stabilisce, il ping continuerà a non funzionare finché non verrà abilitato nella policy.

## 12. Segmentazione con VNET Peering



L'obiettivo dell'esercizio è quello di abilitare la segmentazione fra VNET usando VNET peering

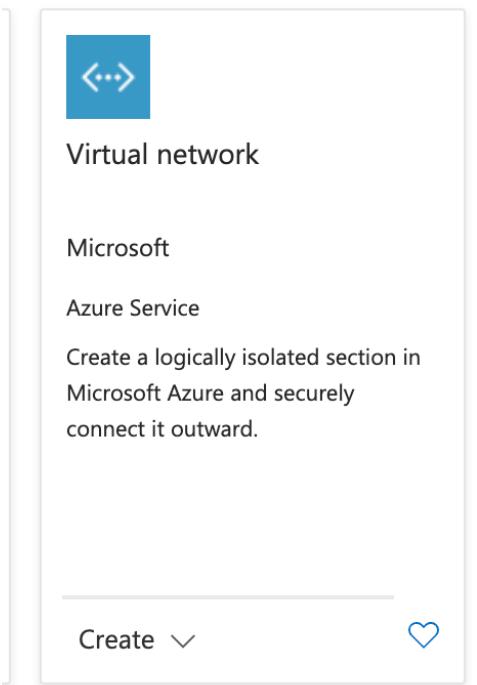
Task dell'esercizio:

- Creazione nuove VNET-spoke2 e VNET-spoke3 con rispettive Protected subnet
- Creazione nuove VM ubuntu all'interno delle due Protected subnet
- Configurazione routing table e VNET Peering
- Configurazione policy sui due nodi hub-fgt per permettere l'SSH
- Verifica traffico

### 12.1. Creazione nuova VNET son una subnet Protected

Dal MarketPlace cercare Virtual Network.

Selezionare Virtual Network e fare “Create > Virtual Network”



**Scegliere il proprio Resource Group e nominare la VNET come spoke2-<nome resource group>**

## Create virtual network

Basics    Security    IP addresses    Tags    Review + create

benefits of Azure's infrastructure such as scale, availability, and isolation.  
[Learn more.](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	SE-Subscription
Resource group *	fmfm11
	<a href="#">Create new</a>

### Instance details

Virtual network name *	spoke2-abdc22
Region * ⓘ	(Europe) Italy North
	<a href="#">Deploy to an Azure Extended Zone</a>

**Next, Next fino a “IP addresses”**

## Configurare come da immagine la subnet 172.16.140.0/22 e creare nuova subnet con nome “protectedsubnet” con indirizzamento 172.16.141.0/24

Home > fmfm11 > Marketplace >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets virtual network address space into smaller ranges for use by your applications. When you deploy resources into the subnet, it assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space | ▾

172.16.140.0/22 Delete

This address prefix overlaps with virtual network 'BHATI-SPOKE-VNET'. If you intend to peer these virtual networks, change the address space. [Learn more](#)

172.16.140.0 /22

172.16.140.0 - 172.16.143.255 1,024 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway

### Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose ...

Default

Name \* ...

protectedsubnet

#### IPv4

Include an IPv4 address space

IPv4 address range \* ...

172.16.140.0/22

172.16.140.0 - 172.16.143.255

Starting address \* ...

172.16.141.0

Size ...

/24 (256 addresses)

Subnet address range ...

172.16.141.0 - 172.16.141.255

#### IPv6

Include an IPv6 address space

This virtual network has no IPv6 address ranges.

#### Private subnet PREVIEW

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound) ...

## Review + Create -> Create

Ripetere la operazione creare una nuova VNET, nominarla spoke3-<nome resource group> con range 172.16.144.0/22 e creare una nuova protected subnet in questa VNET con indirizzamento 172.16.145.0/24:

## Add a subnet

X

select services later. [Learn more ↗](#)

Subnet purpose ⓘ

Default

Name \* ⓘ

protectedsubnet

### IPv4

Include an IPv4 address space

IPv4 address range \* ⓘ

172.16.144.0/22

172.16.144.0 - 172.16.147.255

Starting address \* ⓘ

172.16.145.0

Size ⓘ

/24 (256 addresses)

Subnet address range ⓘ

172.16.145.0 - 172.16.145.255

### IPv6

Include an IPv6 address space  This virtual network has no IPv6 address ranges.

#### Private subnet PREVIEW

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more ↗](#)

Enable private subnet (no default outbound access)

Add

Cancel

↗ Give feedback

## 12.2. Creazione nuove VM all'interno delle nuove VNET

Installare un nuovo server spoke-ubuntu-04.

Tornare nella Home della console AZURE e entrare nel Marketplace.

Nel campo search digitare **ubuntu server** e dare invio

Home > Marketplace ...

Get Started Service Providers Management Private Marketplace Private Offer Management My Marketplace Favorites My solutions Recently created Private plans Categories Compute (540) Developer Tools (461)

Selezionare **Ubuntu Server 22.04 -> Create**

ubuntu server

Azure services only

Showing 1 to 20 of 1604 results for 'ubuntu server'. [Clear search](#)

 Ubuntu Server 22.04 LTS Canonical Virtual Machine Linux For The Cloud  

 Ubuntu Server 20.04 LTS Canonical Virtual Machine Linux For The Cloud  

Virtual machine name \*  ✓

Region \*  ↗

Availability options  ↗

Zone options  ↗

Availability zone \*  ↗

Security type  ↗

Configure security features

Image \*  ↗

Compilare i parametri scorrendo le opzioni fino in fondo

Compilare i parametri come da figura

Run with Azure Spot discount ⓘ

Size \* ⓘ Standard\_B1ms - 1 vcpu, 2 GiB memory (\$17.52/month) [See all sizes](#)

Enable Hibernation ⓘ    
 ⚠️ Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more ↗](#)

**Administrator account**

Authentication type ⓘ  Password

Username \* ⓘ abcd22

Password \* ⓘ ..... Confirm password \* ⓘ .....

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \* ⓘ  None  Allow selected ports

Select inbound ports Select one or more ports

⚠️ All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

< Previous Next : Disks > Review + create

**Impostare password**

**No inbound ports**

**NEXT**

**NEXT**

## Lasciare le impostazioni di default nella sezione Disk - NEXT

Subnet \* ⓘ protectedsubnet (172.16.141.0/24) [Manage subnet configuration](#)

Public IP ⓘ None [Create new](#)

NIC network security group ⓘ  None  Basic  Advanced

Delete NIC when VM is deleted ⓘ

Enable accelerated networking ⓘ  The selected VM size does not support accelerated networking.

## Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more ↗](#)

Load balancing options ⓘ  None  Azure load balancer

## Networking

Compilare i parametri di rete come da figura

Selezionare

La nuova spoke-vnet

ProtectedSubnet

No Public IP

**Review + create**

**Create**

Ripetere le stesse operazioni per una nuova VM da nominare come spoke-ubuntu-05 e posizionarla nella subnet protected subnet della VNET Spoke3

### 12.3. Creazione nuova Route Table da associare alle nuove Subnet

Su MarketPlace cercare Route Table

The screenshot shows the Azure Marketplace search results for 'route table'. A search bar at the top contains the text 'route table'. Below it, a filter section has a checked checkbox for 'Azure services only'. The search results list one item: 'Route table' by Microsoft, which is described as an Azure Service. It explains that route tables control traffic direction in a virtual network. At the bottom of the card, there are 'Create' and 'Heart' (like) buttons.

route table

Azure services only

Showing 1 to 1 of 1 results for 'route table' with 1 selected filters. [Clear](#)

Route table

Microsoft

Azure Service

Use route tables to control how traffic is directed in a virtual network.

Create

Heart

## Create Route Table

Dare il nome RTspokeVNET-<nomeRG>

### Instance details

Region *	<input type="text" value="Italy North"/>	
Name *	<input type="text" value="RTspokeVNET-abcd22"/>	
Propagate gateway routes *	<input checked="" type="radio"/> Yes <input type="radio"/> No	

### Review and Create, Create

**Una volta create selezionare “Go to Resource”**

**Selezionare Settings, Routes e Add per aggiungere una rotta che inoltra tutto il traffico verso il loadbalancer interno della VNET HUB:**

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. [Learn more ↗](#)

Route name \*

Destination type \*

Destination IP addresses/CIDR ranges \*

Next hop type \*

Next hop address \*

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.

Add

Give feedback

Sul menu a sinistra selezionare “Subnets” e associare la subnet “protected subnet” dalla VNET spoke2-abcd22 e della VNET spoke3-abcd22.

## Associate subnet

RTspokeVNET-fmfm11

Virtual network (i)

spoke2-fmfm11 (fmfm11) ▼

Subnet \* (i)

protectedsubnet ▼

Fare OK

### 12.4. Configurazione VNET Peering

Tramite il VNET peering fra le VNET HUB e le due VNET spoke2 e spoke3, le subnet delle VNET Spoke saranno conosciute dal HUB e viceversa.

Selezionare la VNET HUB

Su Settings, Peerings selezionare Add

Configurare come da immagine, impostare la VNET spoke2-abcd22

### Remote virtual network summary

Peering link name *	hubspokepeering
Virtual network deployment model ⓘ	<input checked="" type="radio"/> Resource manager <input type="radio"/> Classic
I know my resource ID ⓘ	<input type="checkbox"/>
Subscription *	SE-Subscription
Virtual network *	spoke2-fmfm11 (fmfm11)

### Remote virtual network peering settings

- Allow 'spoke2-fmfm11' to access 'hub-fmfm11' ⓘ
- Allow 'spoke2-fmfm11' to receive forwarded traffic from 'hub-fmfm11' ⓘ
- Allow gateway or route server in 'spoke2-fmfm11' to forward traffic to 'hub-fmfm11' ⓘ

Continuando fino in fondo configurare il peering anche lato spoke

### Local virtual network summary

Peering link name *	spokehubpeeing
---------------------	----------------

### Local virtual network peering settings

- Allow 'hub-fmfm11' to access 'spoke2-fmfm11' ⓘ
- Allow 'hub-fmfm11' to receive forwarded traffic from 'spoke2-fmfm11' ⓘ
- Allow gateway or route server in 'hub-fmfm11' to forward traffic to 'spoke2-fmfm11' ⓘ
- Enable 'hub-fmfm11' to use 'spoke2-fmfm11's' remote gateway or route server ⓘ

Add

Cancel

Fare Add

Ripetere per la VNET Spoke3.

## 12.5. Impostare il routing sui due Fortigate HUB

Il next Hop verso le subnet 172.16.141.0/24 e 172.16.145.0/24 dovrà essere il system route interno 172.16.136.65. Impostare le rispettive rotte statiche su entrambi i firewall HUB.

Creare la regola firewall per permettere il traffico fra VM Spoke4 e VM Spoke5

Su entrambi i firewall HUB creare la regola per permettere il traffico SSH da protectednetwork Spoke3 alla protectedsubnet Spoke4

Creare nuovi oggetti address per le vm Ubuntu Spoke4, con indirizzo 172.16.141.4 e Ubuntu Spoke5, con indirizzo 172.16.145.4.

Per abilitare il traffico creare la policy sui due fortigate hub con i relativi oggetti in modo bidirezionale.

The screenshot shows the configuration interface for a policy named "spoke-spoke". The policy is set to "ACCEPT" and has a "Standard" type. It applies to "port2" on both incoming and outgoing interfaces. The "Source & Destination" tab is selected, showing bidirectional traffic between "spoke-ubuntu-04" and "spoke-ubuntu-05". The "Destination" section also includes "ALL". The "Firewall/Network Options" tab is at the bottom, showing "Flow-based" inspection mode and NAT enabled.

Name	spoke-spoke
Schedule	always
Action	✓ ACCEPT
Type	Standard
Incoming interface	port2
Outgoing interface	port2
Source & Destination	
Source	spoke-ubuntu-04 spoke-ubuntu-05 +
User/group	+
Security posture tag	(radio button)
Destination	spoke-ubuntu-04 spoke-ubuntu-05 +
Service	ALL +
Firewall/Network Options	
Inspection mode	Flow-based
NAT	(checkbox)

spoke-ubuntu-04: 172.16.141.4

spoke-ubuntu-05: 172.16.145.4

Non è necessario abilitare il NAT poiché le sessioni est-ovest attraversano solo il bilanciatore interno.

## 12.6. TEST

Accedere in ssh a hub-ubuntu-01 e da qui a spoke-ubuntu-04 (ssh 172.16.141.4).

Da spoke-ubuntu-04 fare ping verso spoke-ubuntu-05 (172.16.145.4).

Provare a fare anche SSH da spoke-ubuntu-04 verso spoke-ubuntu-05.

Cambiare la regola per permetter solo SSH e verificare che il ping smette di funzionare.

## 13. Rimozione risorse

Prima di concludere il LAB rimuovere tutte le risorse create.

Dalla home selezionare il proprio resource group

Home > abcd22 < ...

Search

Overview

+ Create Manage view Refresh

^ Essentials

Subscription (move) : SE-Subscription

Subscription ID : cf72478e-c3b0-4072-8f60-41d037c1d9e9

Tags (edit) : CreatedOnDate : 2024-07-10T09:31:16.2728649Z

Resources Recommendations (2)

Filter for any field... Type equals all Location equals all

Show hidden types ⓘ

Name ↑

- ARSabcd22
- hub-abcd22
- hub-abcd22-ip
- hub-externalloadbalancer
- hub-externalloadbalancer-pip
- hub-fgt-1
- hub-fgt-1-nic1
- hub-fgt-1-nic2
- hub-fgt-1\_disk2\_e19f3cfadcb440599844d300c9fa42
- hub-fgt-1\_OsDisk\_1\_f6bed80a20294cf58692b609757d4f50
- hub-fgt-2
- hub-fgt-2-nic1
- hub-fgt-2-nic2

nel menu in alto selezionare

### Delete resource group

Apply force delete for selected Virtual machines and Virtual machine scale sets ⓘ

Enter resource group name to confirm deletion \*

abcd22

**Delete** **Cancel**

In basso a destra digitare il nome del resource group nella form e selezionare **Delete**