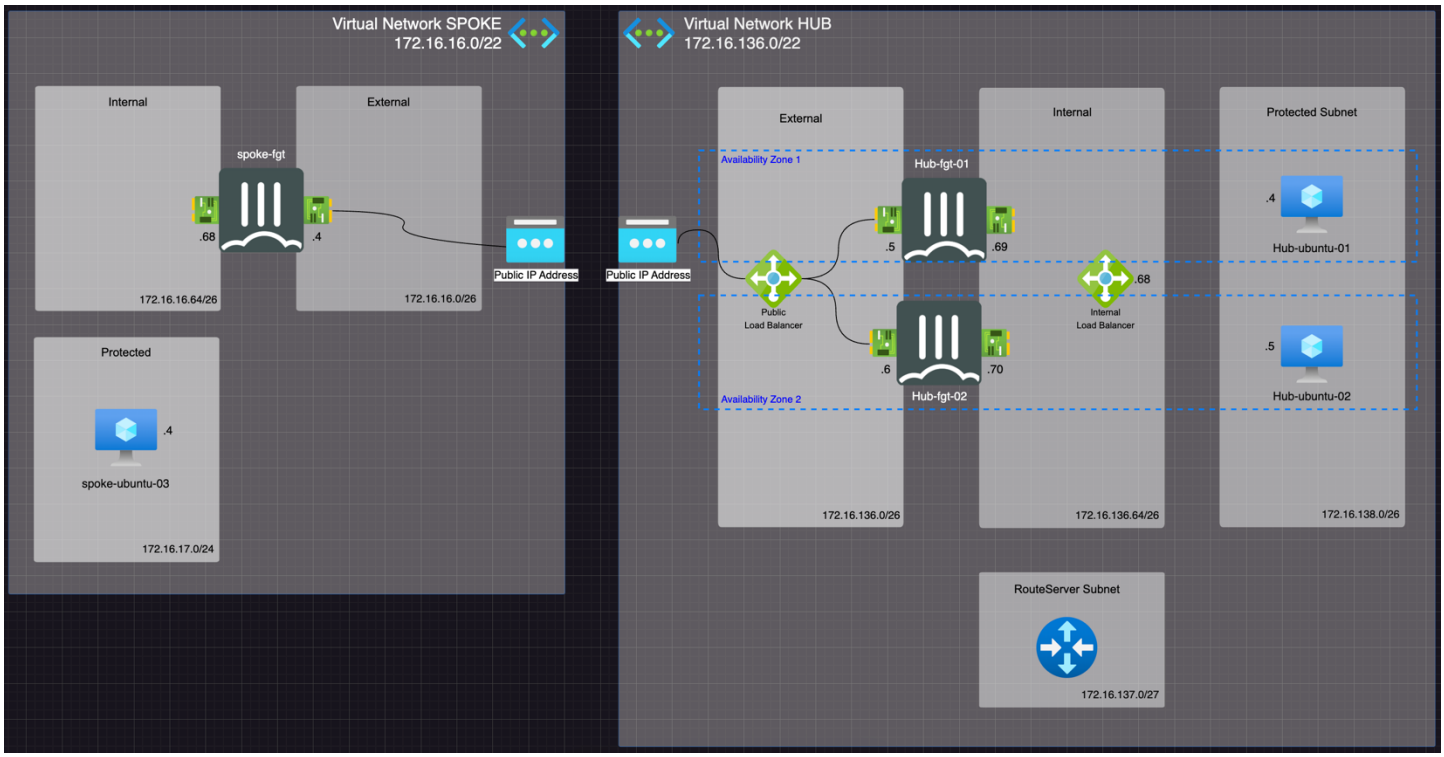
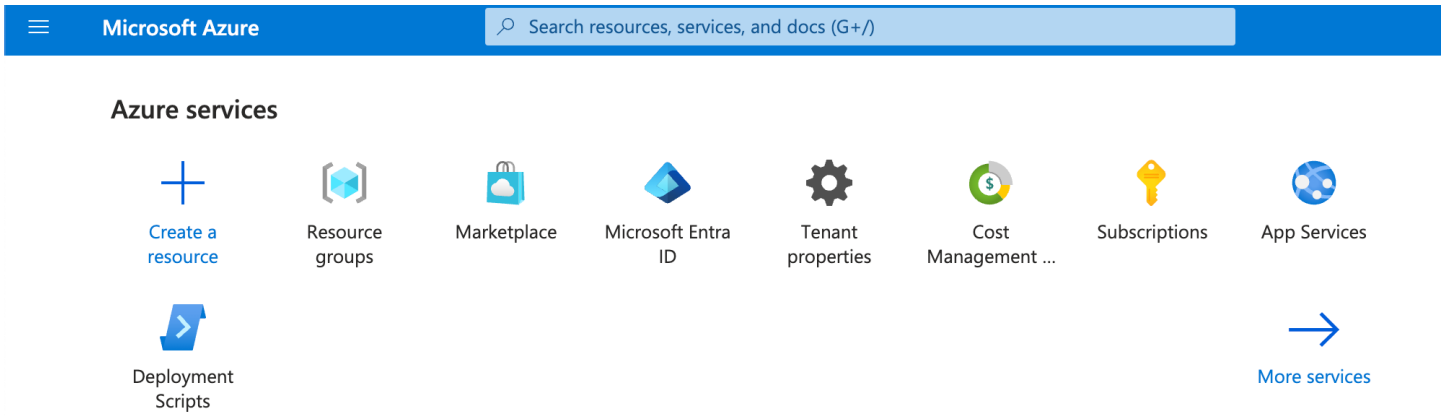
Fortigate @AZURE lab

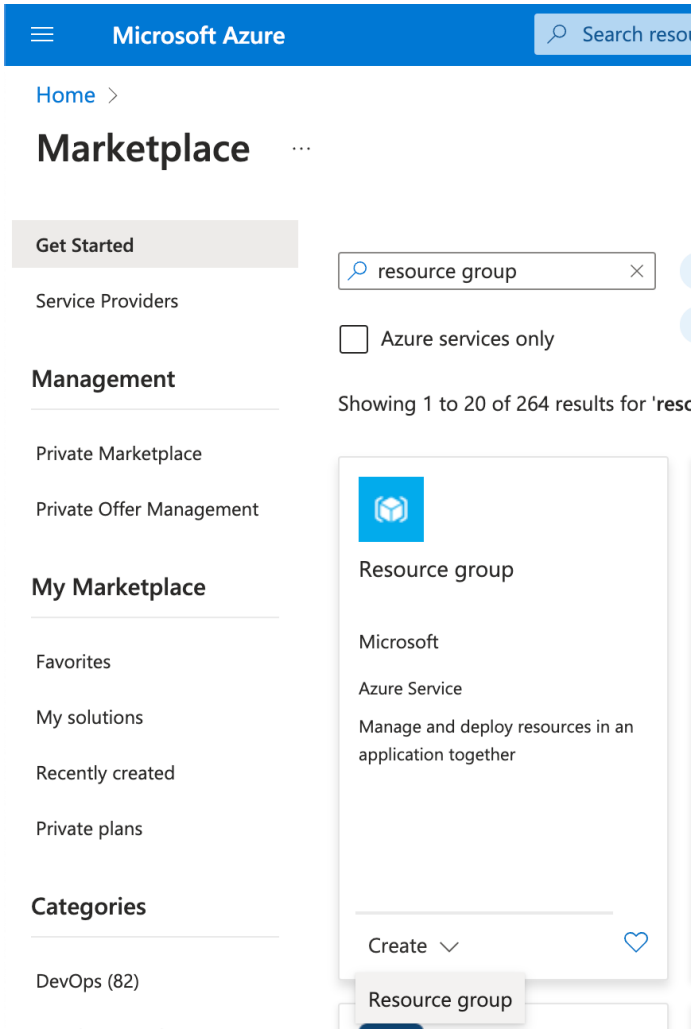

Virtual Network SPOKE
172.16.16.0/22
Internal
External
spoke-fgt
.68
.4
172.16.16.64/26
172.16.16.0/26
Public IP Address
Protected
.4
spoke-ubuntu-03
172.16.17.0/24
Virtual Network HUB
172.16.136.0/22
Public IP Address
External
Internal
Protected Subnet
Availability Zone 1
Hub-fgt-01
.5
.69
.4
Hub-ubuntu-01
Public
Load Balancer
Internal
Load Balancer
.68
.6
.70
.5
Hub-ubuntu-02
Availability Zone 2
Hub-fgt-02
172.16.136.0/26
172.16.136.64/26
172.16.138.0/26
RouteServer Subnet
172.16.137.0/27

1. Creazione Resource Group

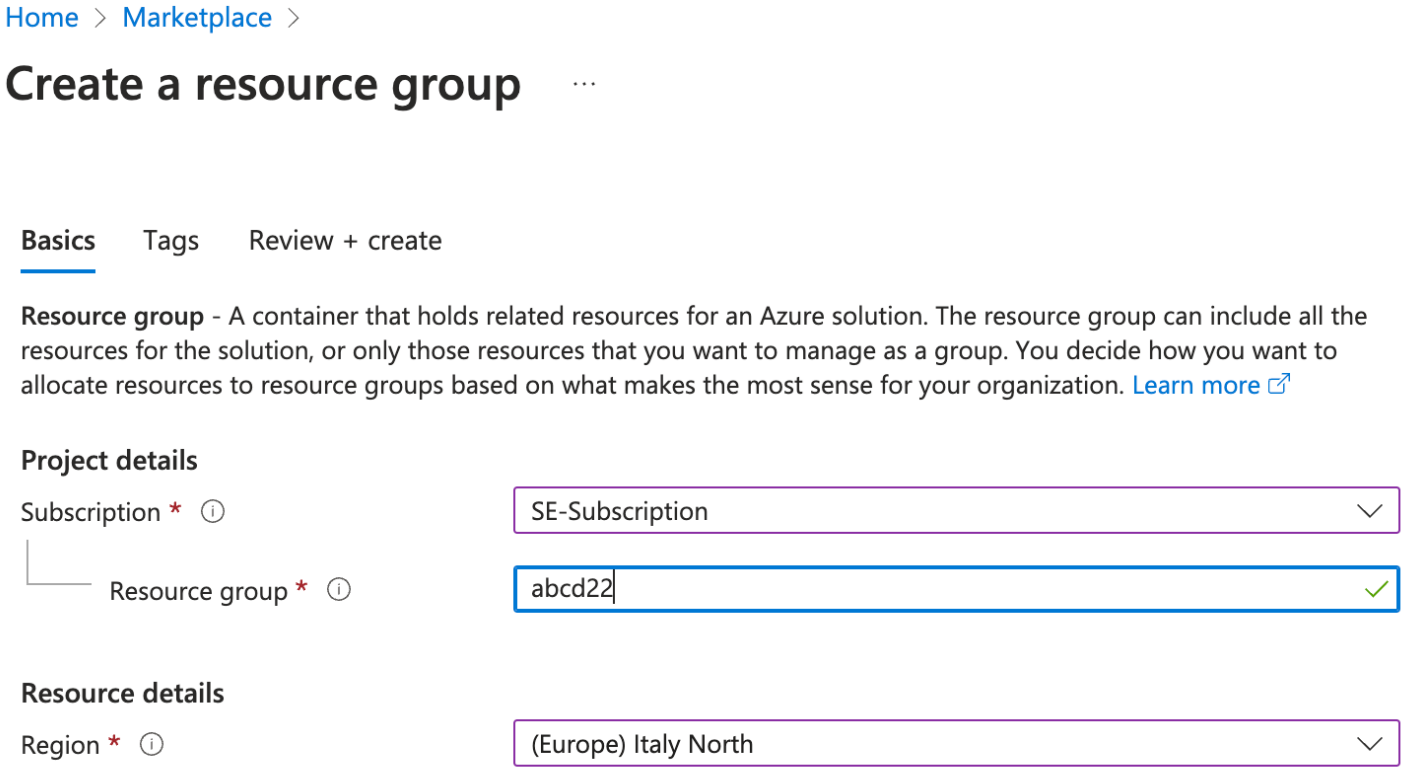
Dalla home del portale Azure -> ***Create a Resource***



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



Create Resource Group



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

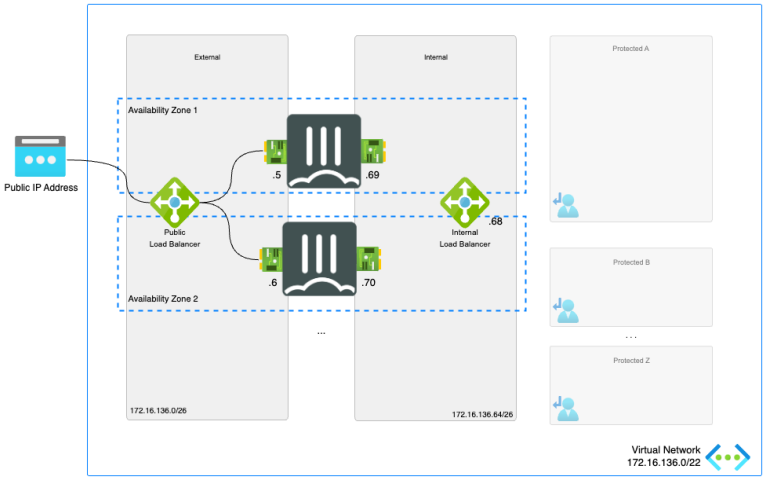
2. HUB - Creazione cluster Fortigate Active/Active

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

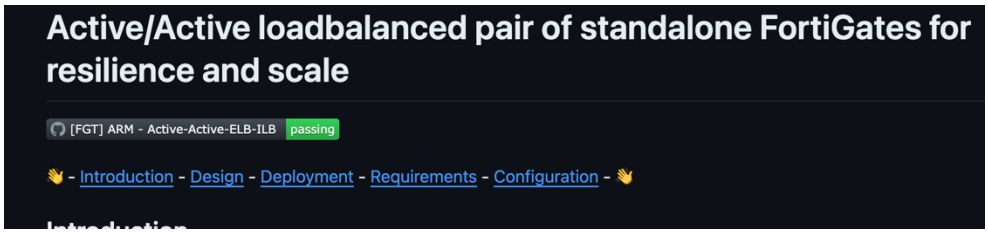
https://github.com/caliaf/AZURE/edit/main/FortiGate/Active-Active-ELB-ILB/

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.

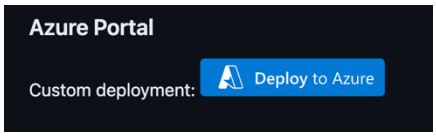
Il template permette la configurazione di diverse opzioni per indirizzare molteplici architetture Active/Active.



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

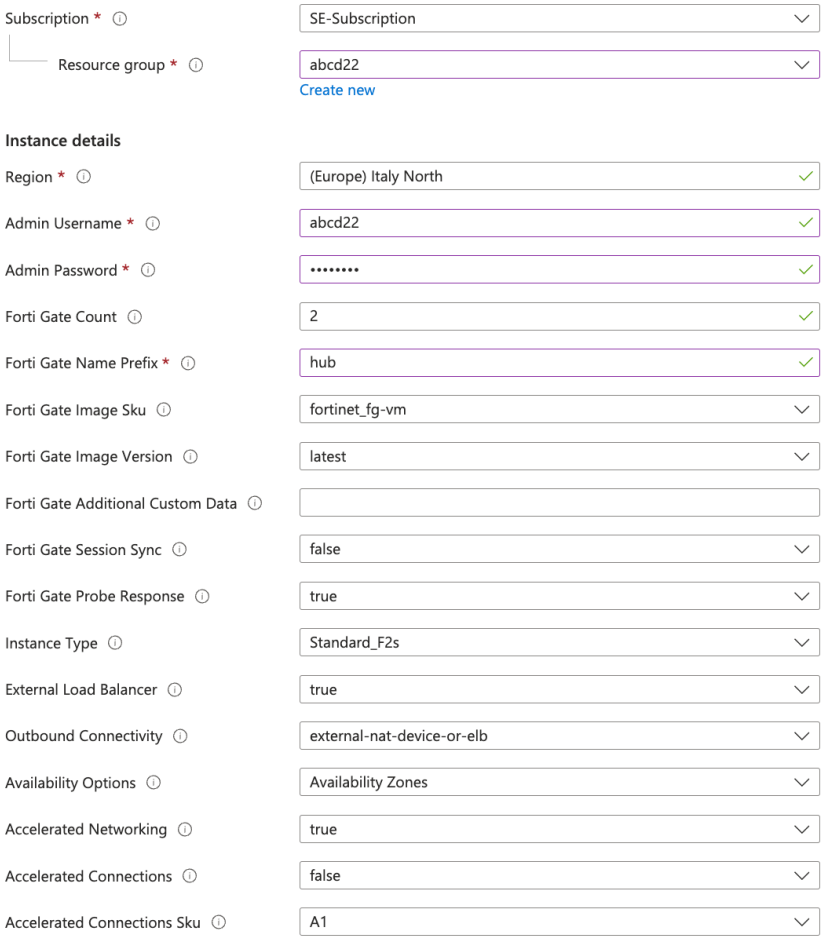


Nerl menu del repository in alto sutto il titolo selezionare ***Deployment***



Selezionare ***Deploy to Azure***

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



Compilare il form come in figura:

Se non già presente selezionare la Subscription del proprio account

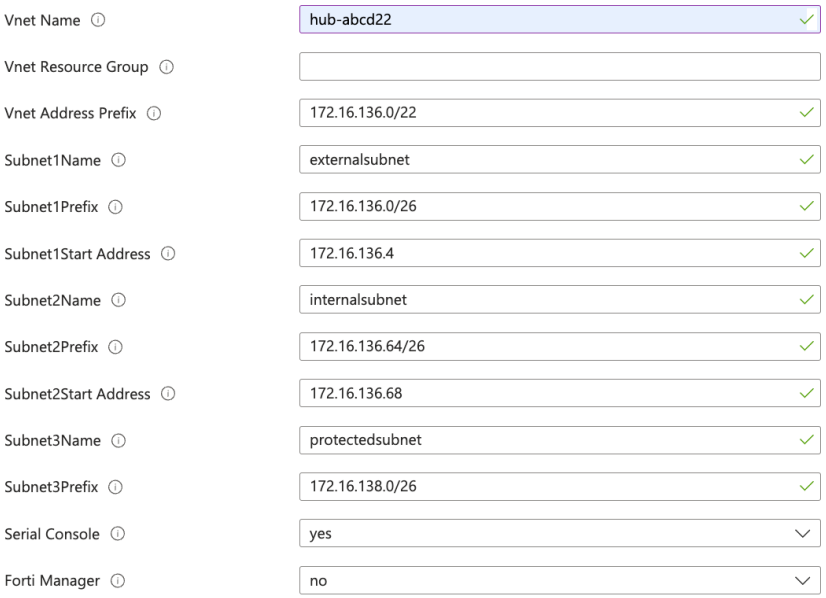
Selezionare il proprio Resource Group creato predentemente

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)

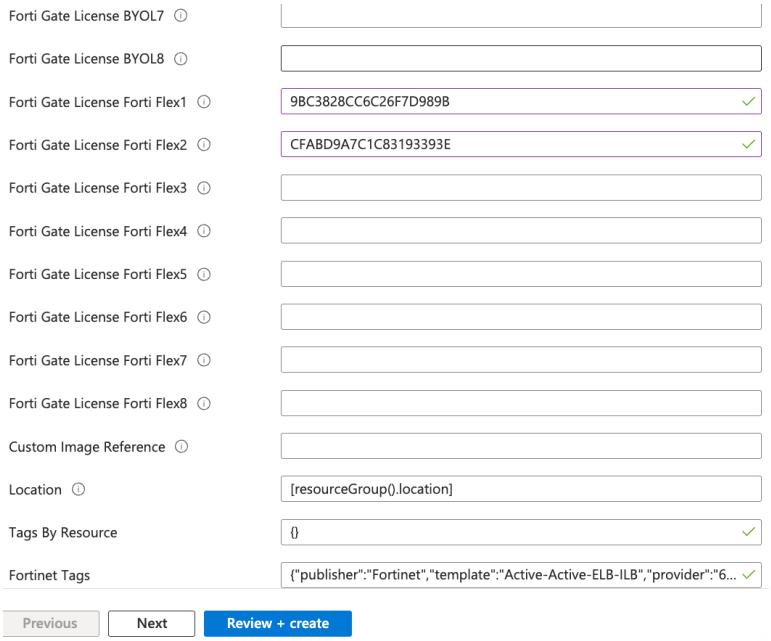
Inserire ***hub*** come prefisso

Scorrere e lasciare le altre impostazioni di Default fino a Vnet Name



Vnet Name : hub-<resource gorup>
(per es. hub-abcd22)

Scorrere e lasciare le impostazioni di default fino a Fortigate License FortiFlex



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***

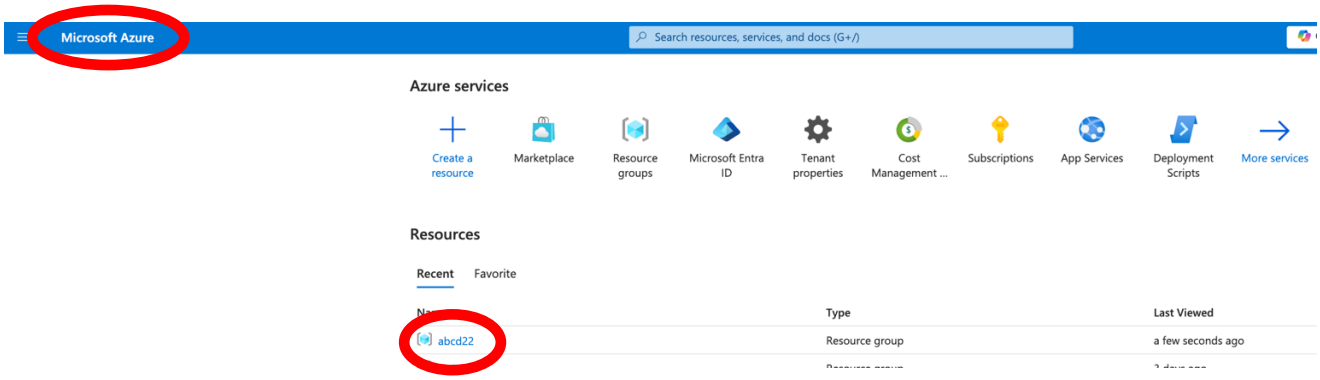
Selezionare ***Create***

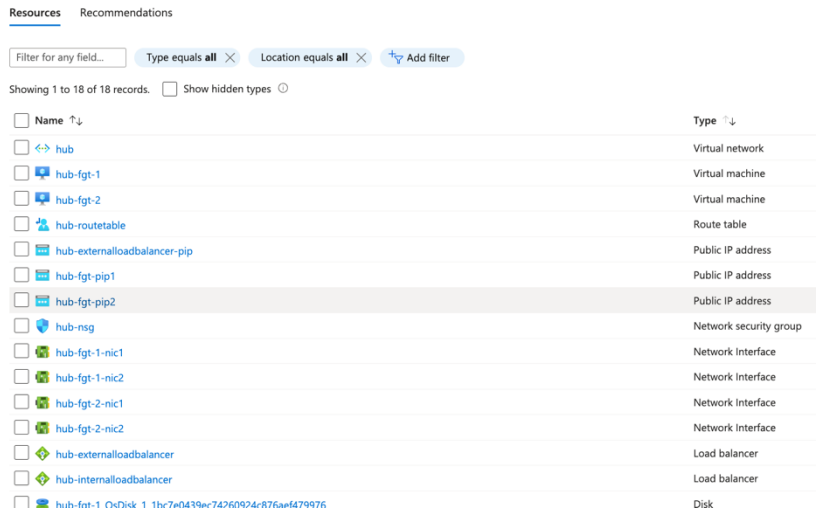
3. HUB - Creazione Azure Route Server

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





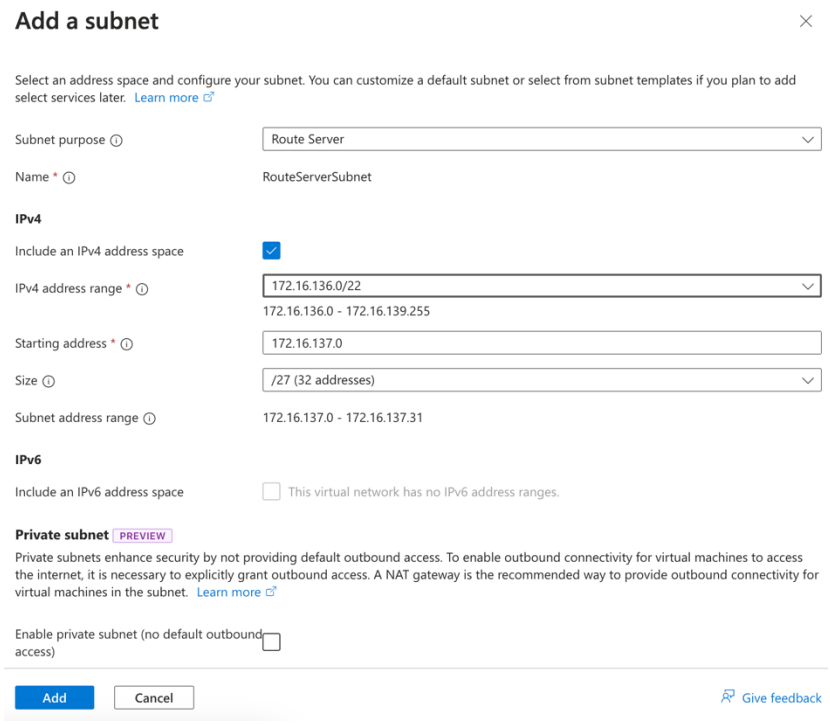
Selezionare il nome della colonna Type per mettere in ordine le risorse

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***



Inerire le opzioni come in figura a fianco:

Subnet purpose: Route Server

Automaticamente viene impostato il nome della subnet.

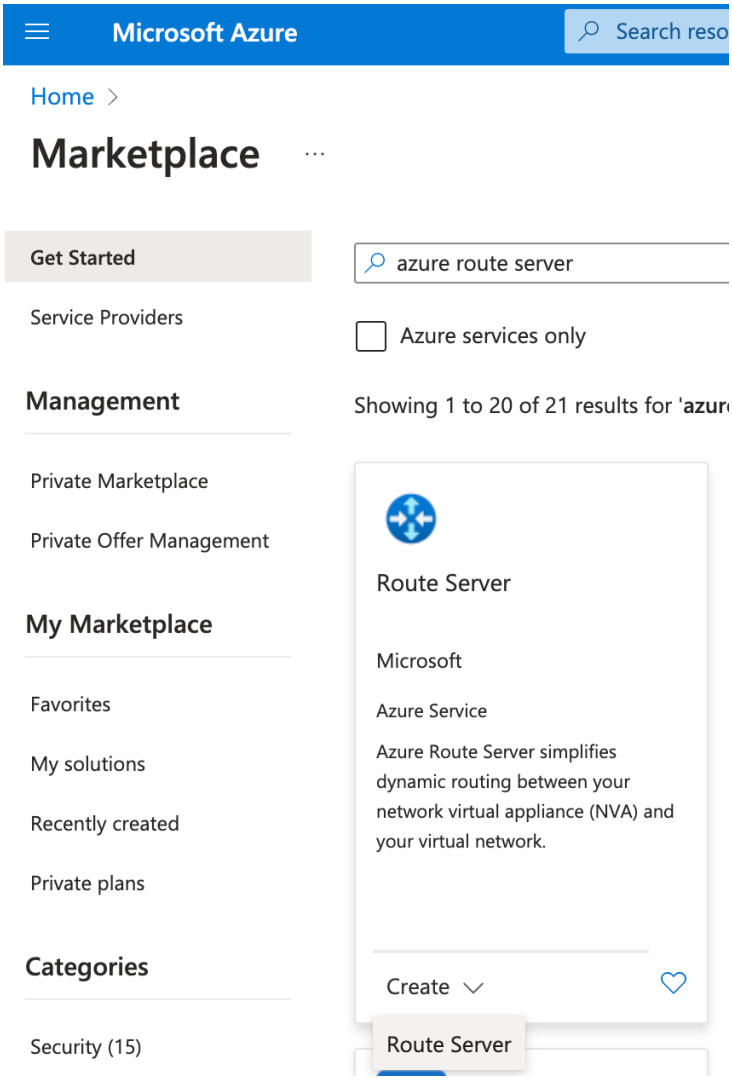
IPV4 address range, lasciare la VNET

Starting Address 172.16.137.0

Size: /27

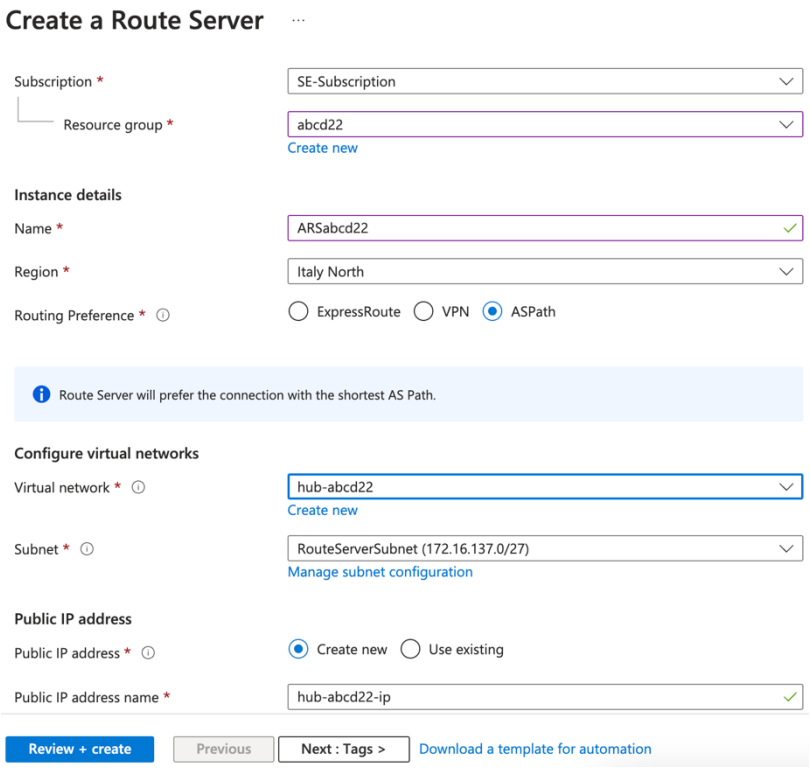
Selezionare ***ADD***

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



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

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



Compilare i parametri come da figura a fianco.

Usare come nome del router

ARS<nome resource group>

Routing Preference: ASPath

Vnet hub e subnet creata precedentemente.

Review + create -> Create

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

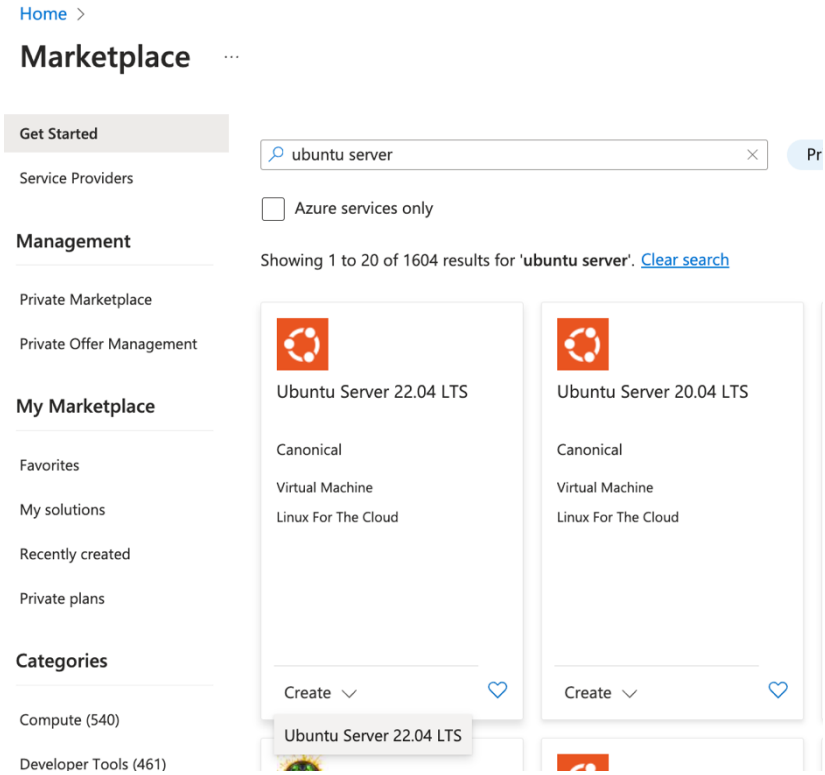
Iniziare a creare nella ProtectedSubnet della vnet HUB una VM Linux che verrà utilizzate per i test.

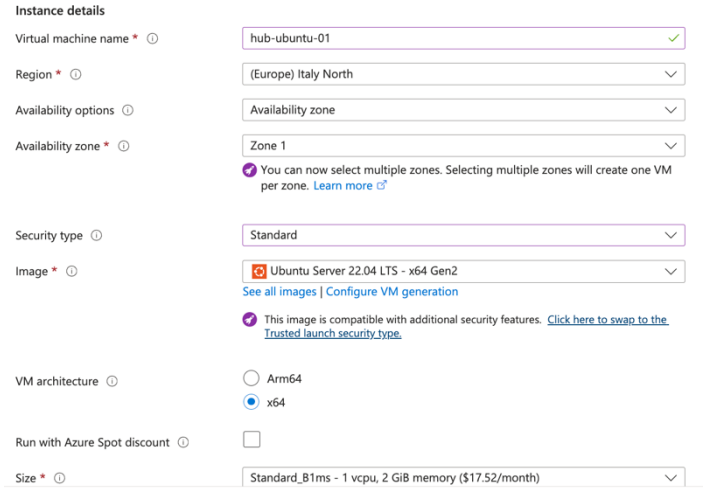
4. HUB - Creazione server Ubuntu01

Tornare nella Home della console Azure e entrare nel Marketplace.

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

Selezionare ***Ubuntu Server 22.04 -> Create***





Compilare i parametri scorrendo le opzioni fino in fondo

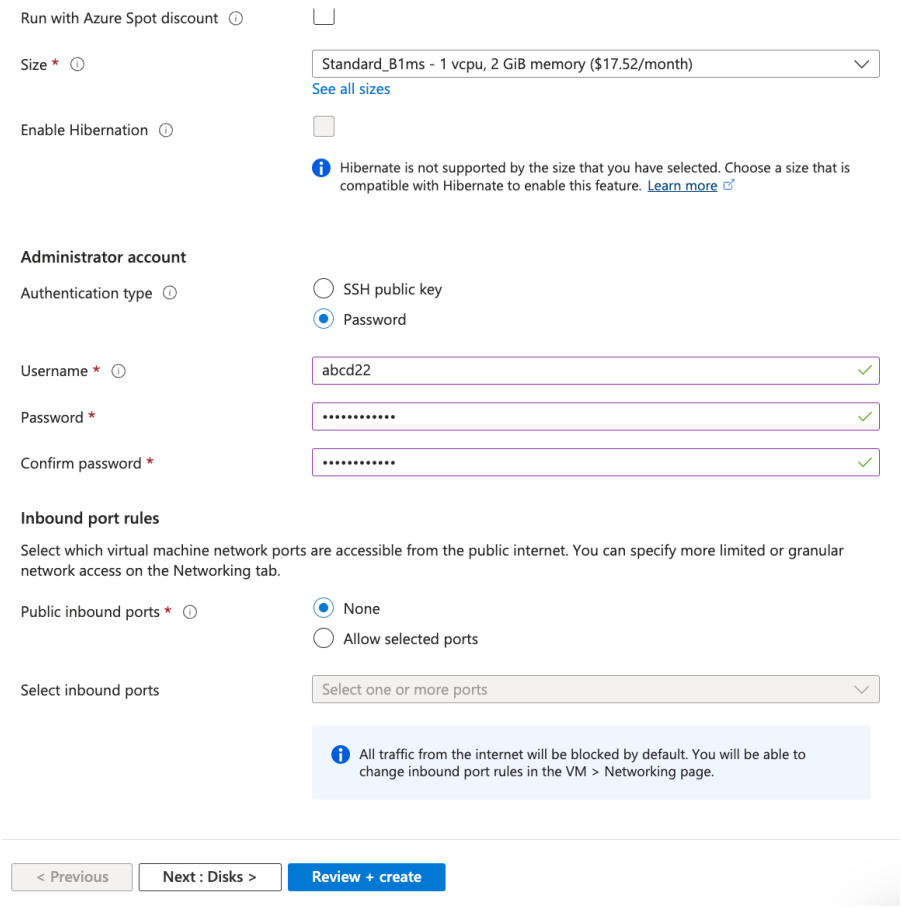
Resource Group : confermare vostro Resource Groupe

VM name: hub-ubuntu-01

Security Type: Standard

Create

Compilare i parametri come da figura



Authentication Type: Password

Impostare username = RG name

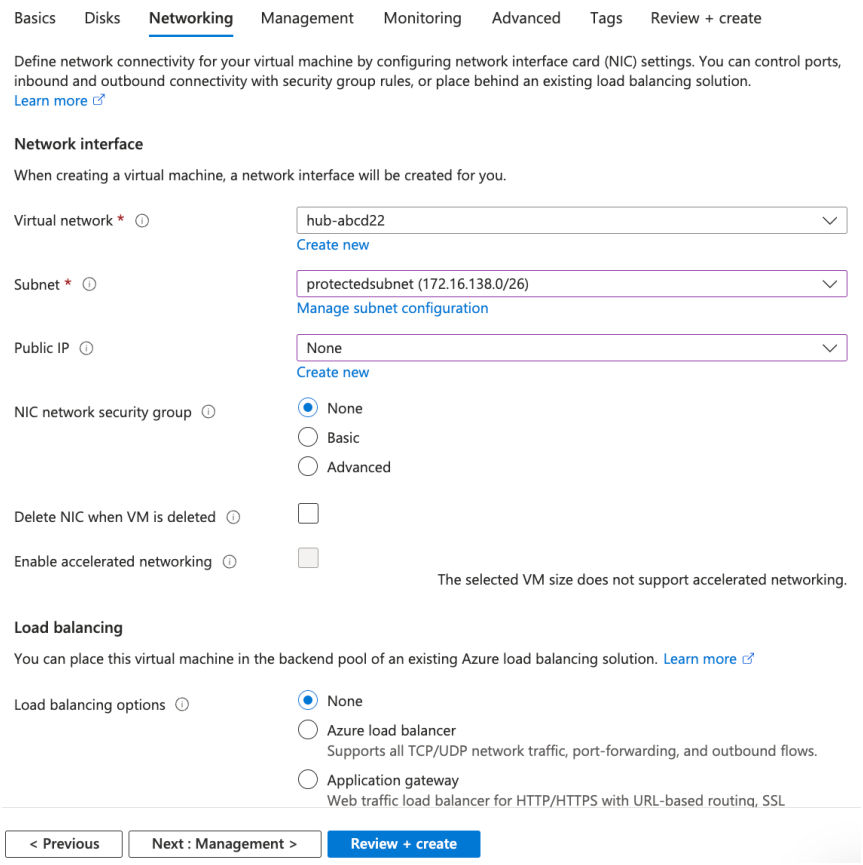
Impostare password

No inbound ports

NEXT

NEXT

Lasciare le impostazioni di default nella sezione Disk - NEXT



Networking

Compilare i parametri di rete come da figura

Selezionare

La propria HUB-vnet

ProtectedSubnet

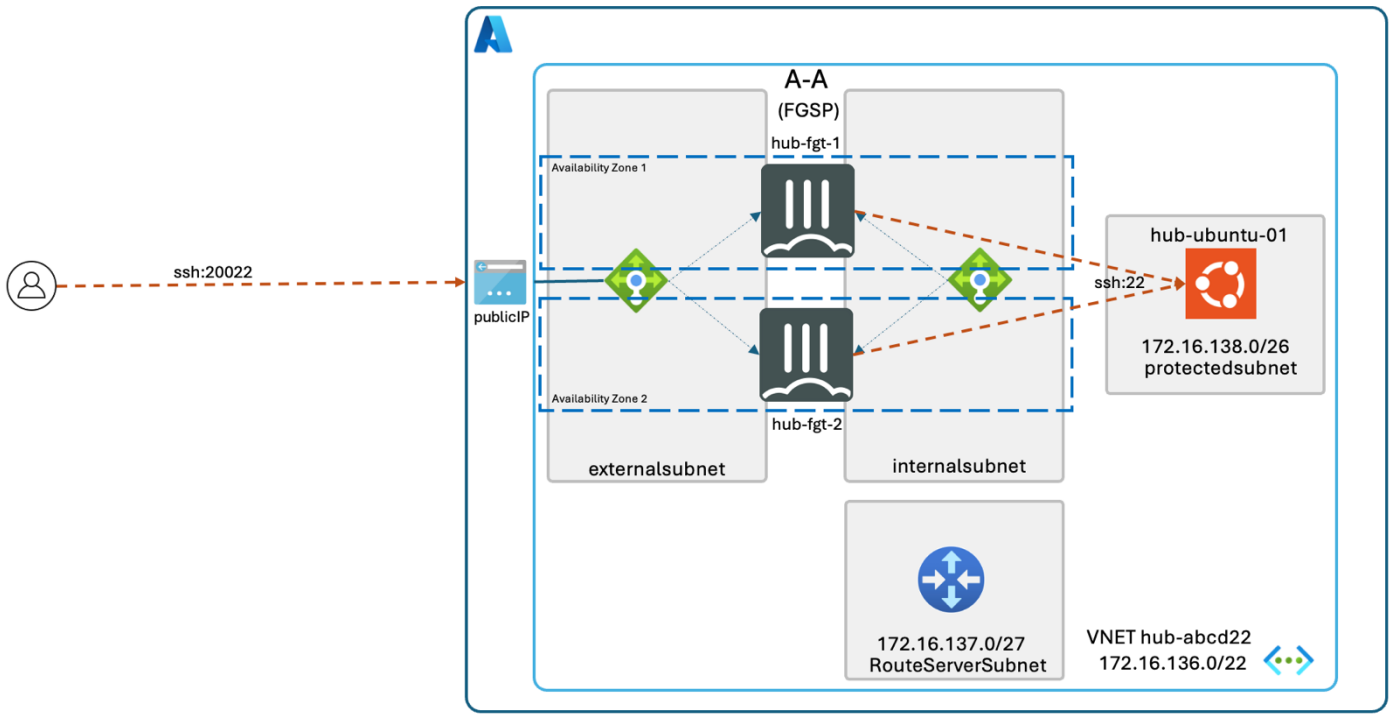
NIC security Group None

No Public IP

Review + create

Create

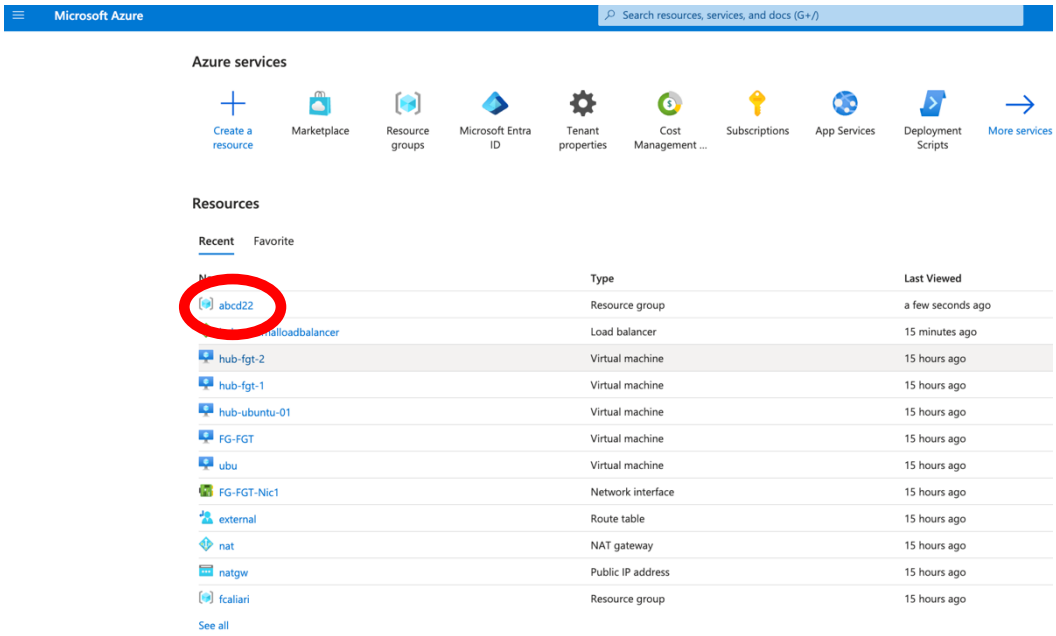
5. HUB - Accesso server Ubuntu01 tramite VIP cluster



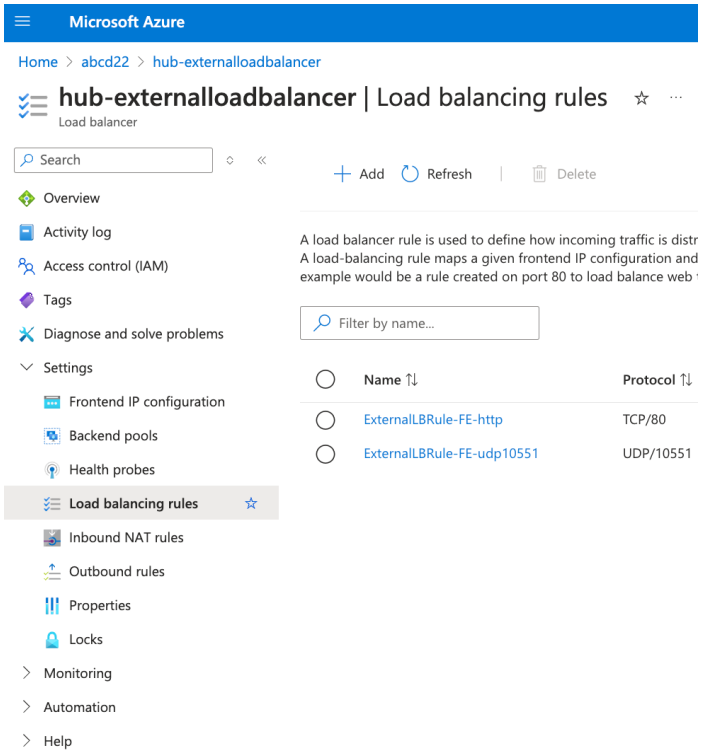
Per abilitare la connessione SSH via internet da client esterno al server Ubuntu occorre completare i seguenti task:

- Creazione regola sul loadbalancer per gestire la porta che verrà utilizzate 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



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

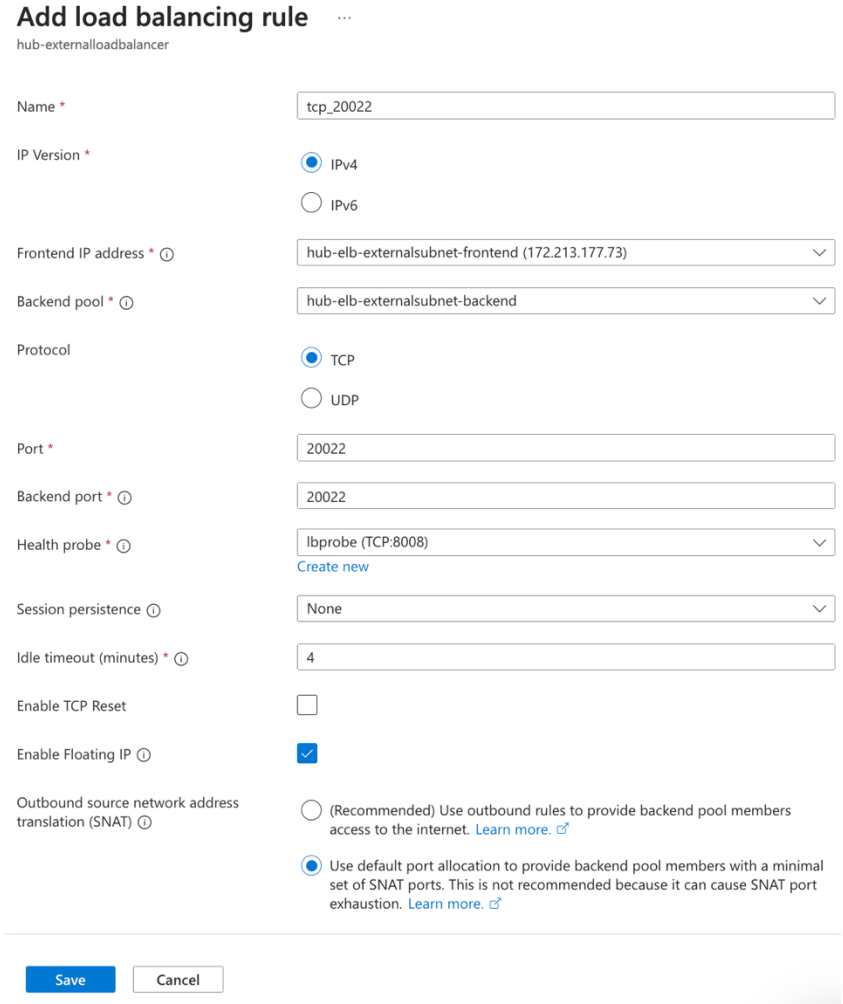


Dal menu selezionare ***Settings***

e

Load balancing rules

Selezionare ***Add***



Compilare i parametri come in figura a fianco.

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

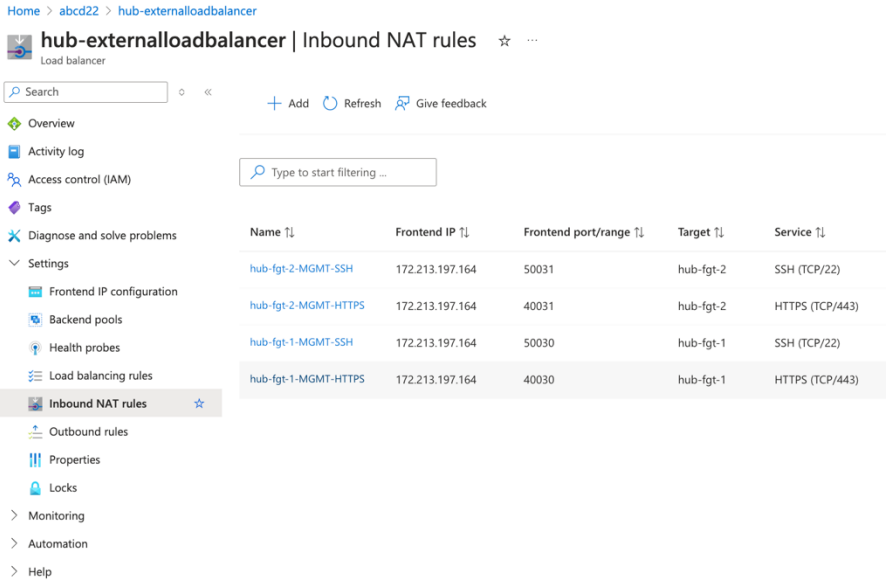
I fortigate vedranno come ip destinatario l'ip pubblico del bilanciatore.

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

Save

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



Gui HTTPS di hub-fg-1: porta 40030

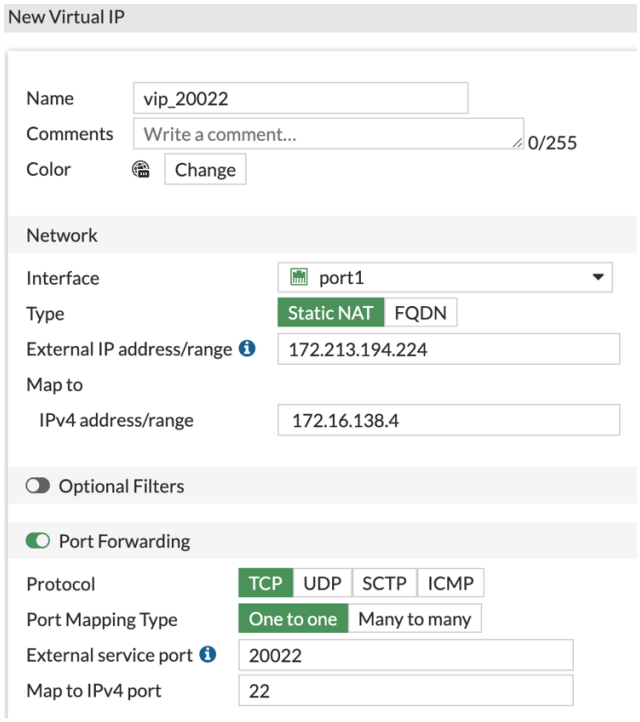
Gui HTTPS di hub-fg-2: porta 40031

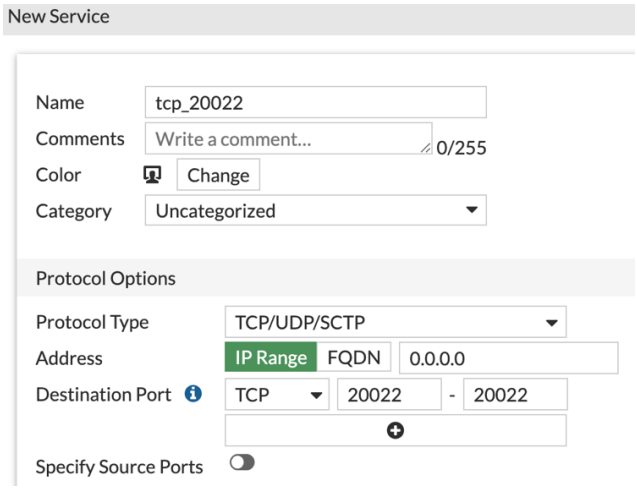
SSH hub-fg-1: porta 50030

SSH hub-fg-2: porta 50031

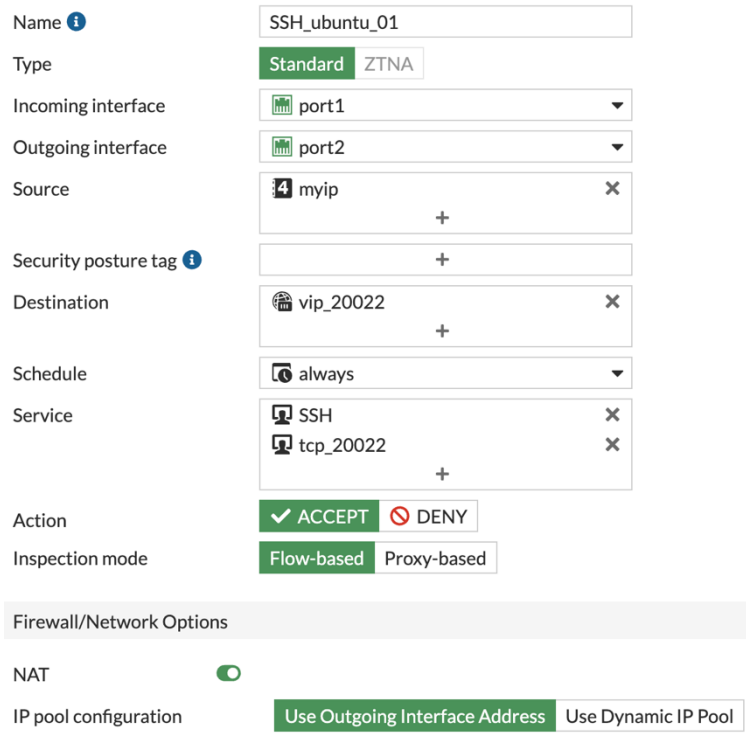
Dopo l'accesso ai Fortigate hub inserire il token FortiFlex se non già configurato al lancio del template.

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



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 poichè 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
```

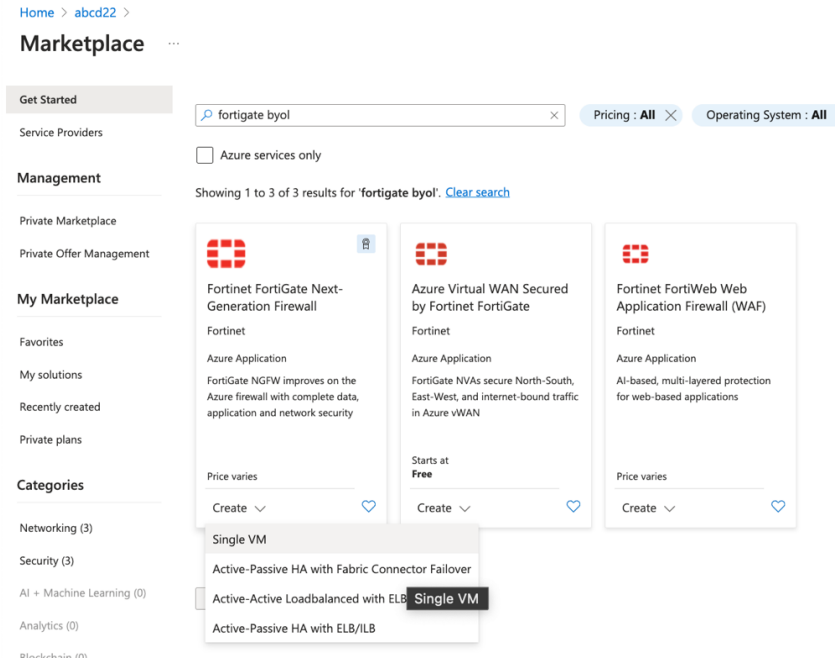
Dall'elenco delle sessioni sul fortigate (Dashboard – Fortiview Sessions) verificare su quale Fortigate il bilanciatore di Azure ha girato la connessione ssh.

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)

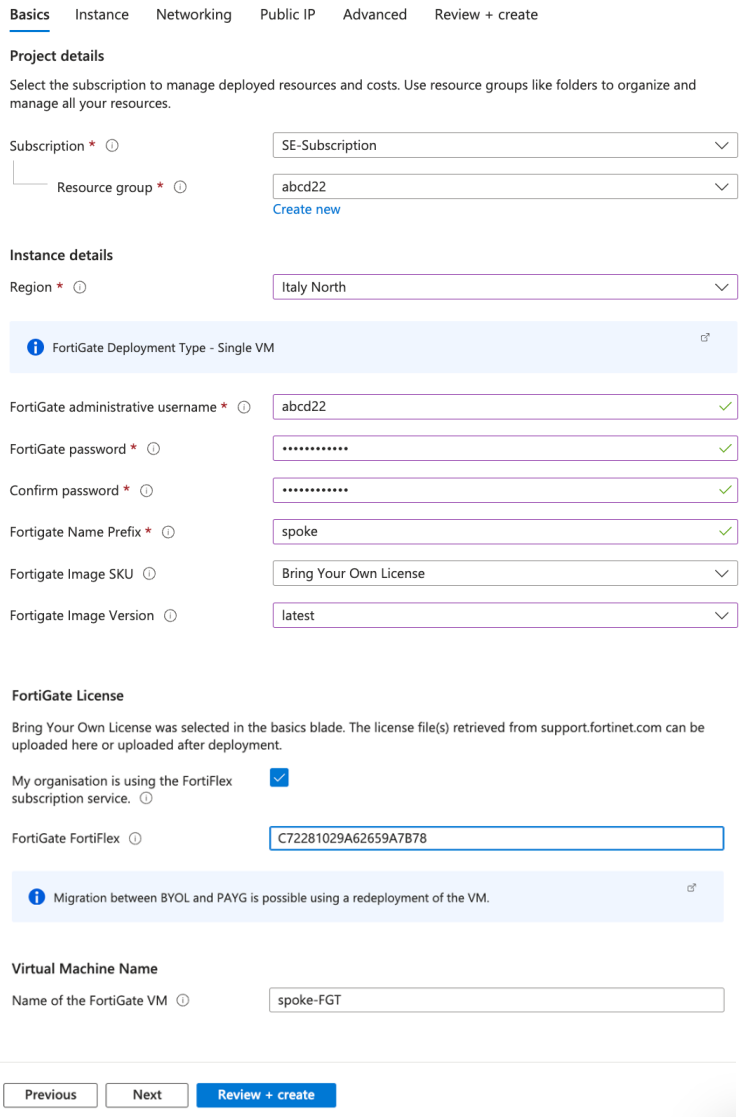
Dalla home della console selezionare Marketplace



Nel campo search digitare ***Fortigate BYOL***

In Fortinet Fortigate Next-Generation Firewall, selezionare

Create -> Single VM

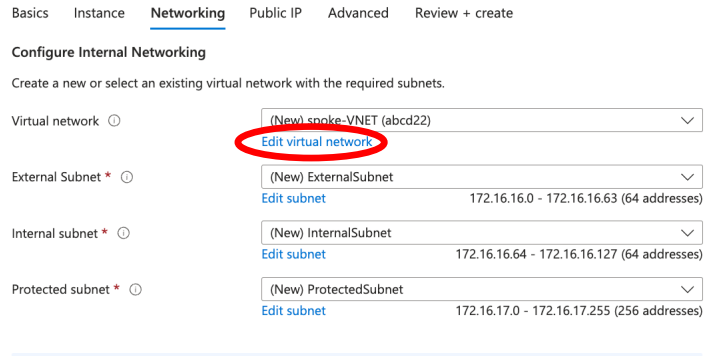


Compilare i parametri come da figura a fianco.

Next

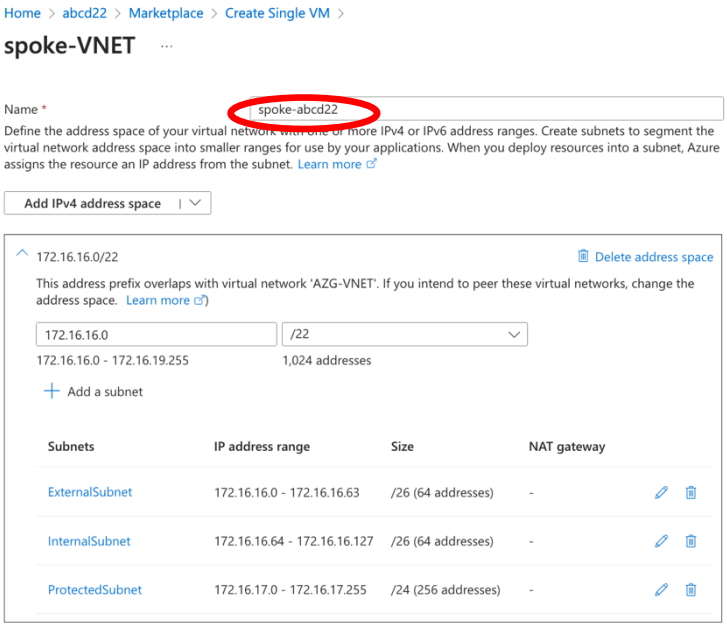
Selezionare Fortiflex e inserire terzo token

Next



Il template crea automaticamente una VNET con 3 subnet.

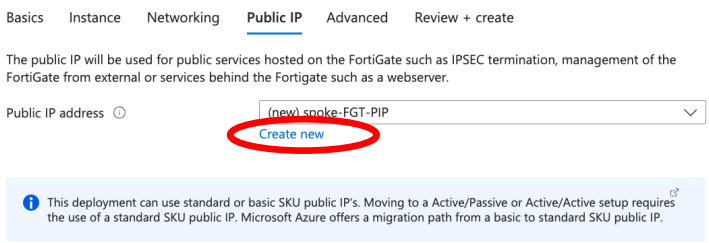
Edit virtual network per modificare il nome della vnet



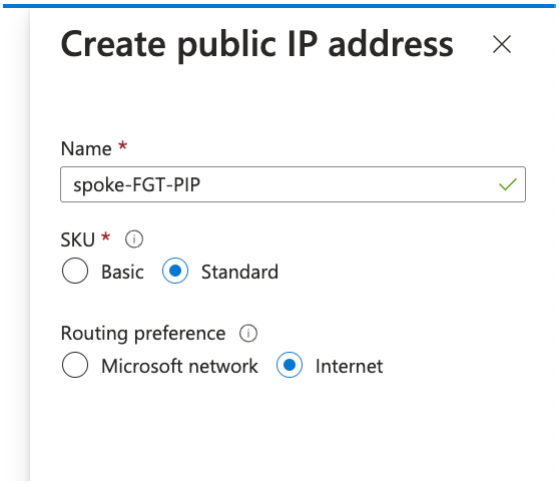
Nel campo nome inserire ***spoke-<nome resource group>***

SAVE

NEXT



Selezionare ***Create new*** per modificare le opzioni del Public IP associato al Fortigate

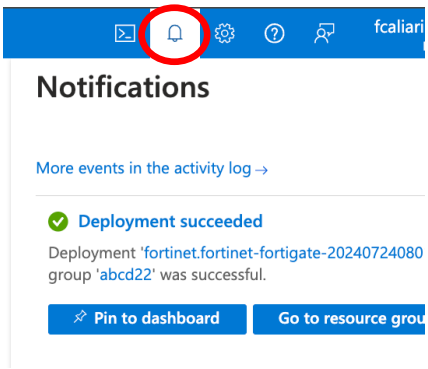


Impostare i parametri come in figura

in basso a destra selezionare ***OK***

Review + create

Create

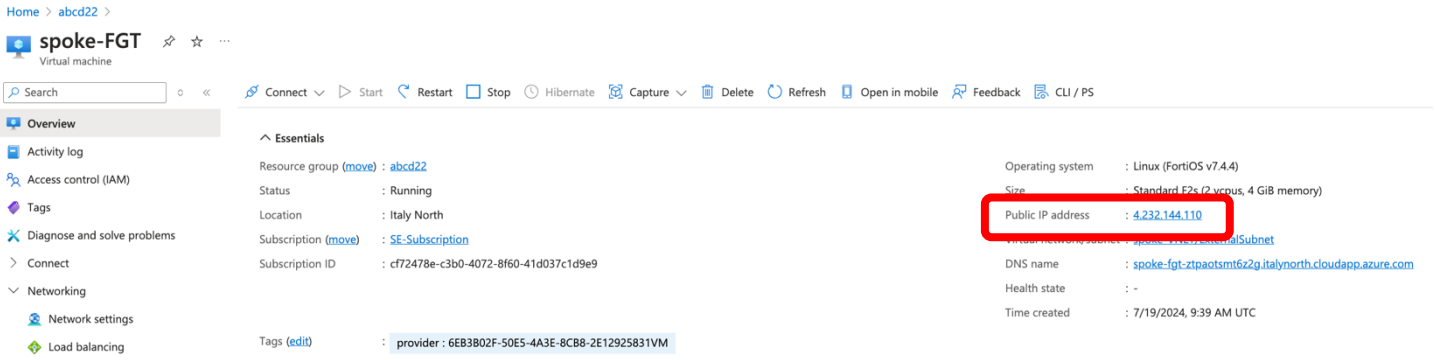


Attendere qualche minuto per permettere al deployment di terminare la creazione di tutti le risorse.

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

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



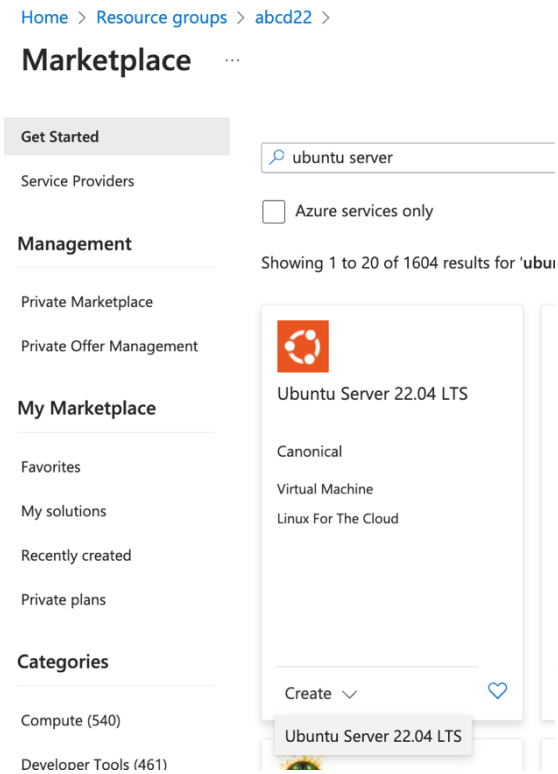
Se non già inserito durante il wizard accedere alla gui https del fortigate e attivare la licenza mediante il token fortiflex (utilizzare il terzo token ricevuto via mail).

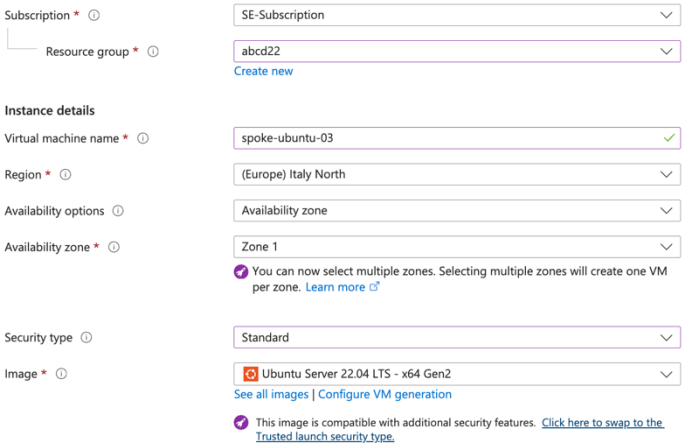
7. SPOKE - Creazione server Ubuntu03

Tornare nella Home della console e entrare nel Marketplace.

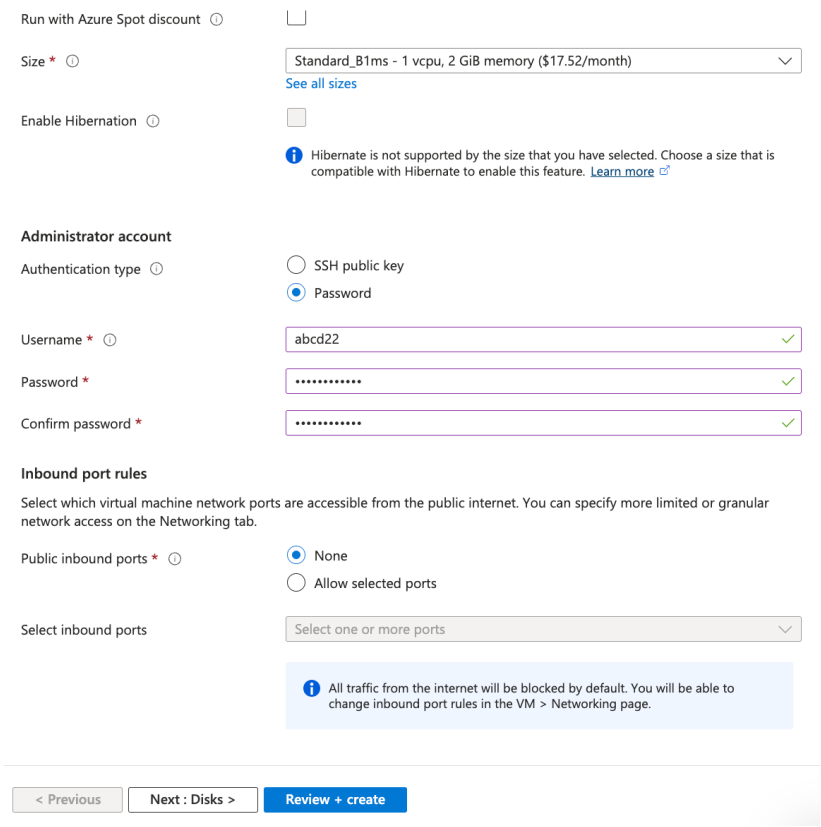
Nel campo search digitare ***ubuntu server*** e dare invio

Selezionare ***Ubuntu Server 22.04 -> Create***





Compilare i parametri scorrendo le opzioni fino in fondo

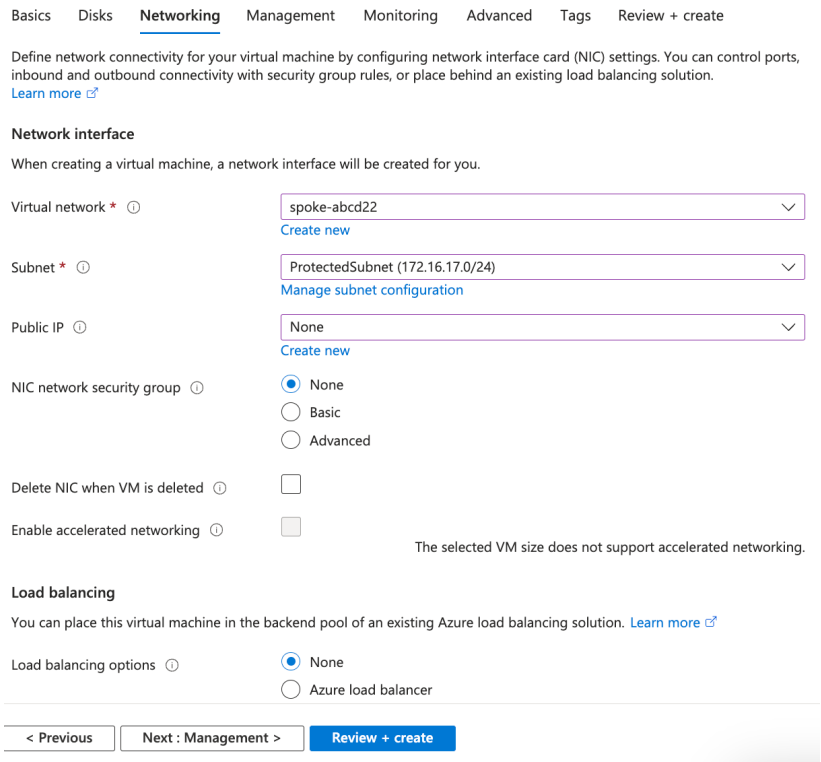


Impostare password

No inbound ports

NEXT

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



Networking

Compilare i parametri di rete come da figura

Selezionare

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

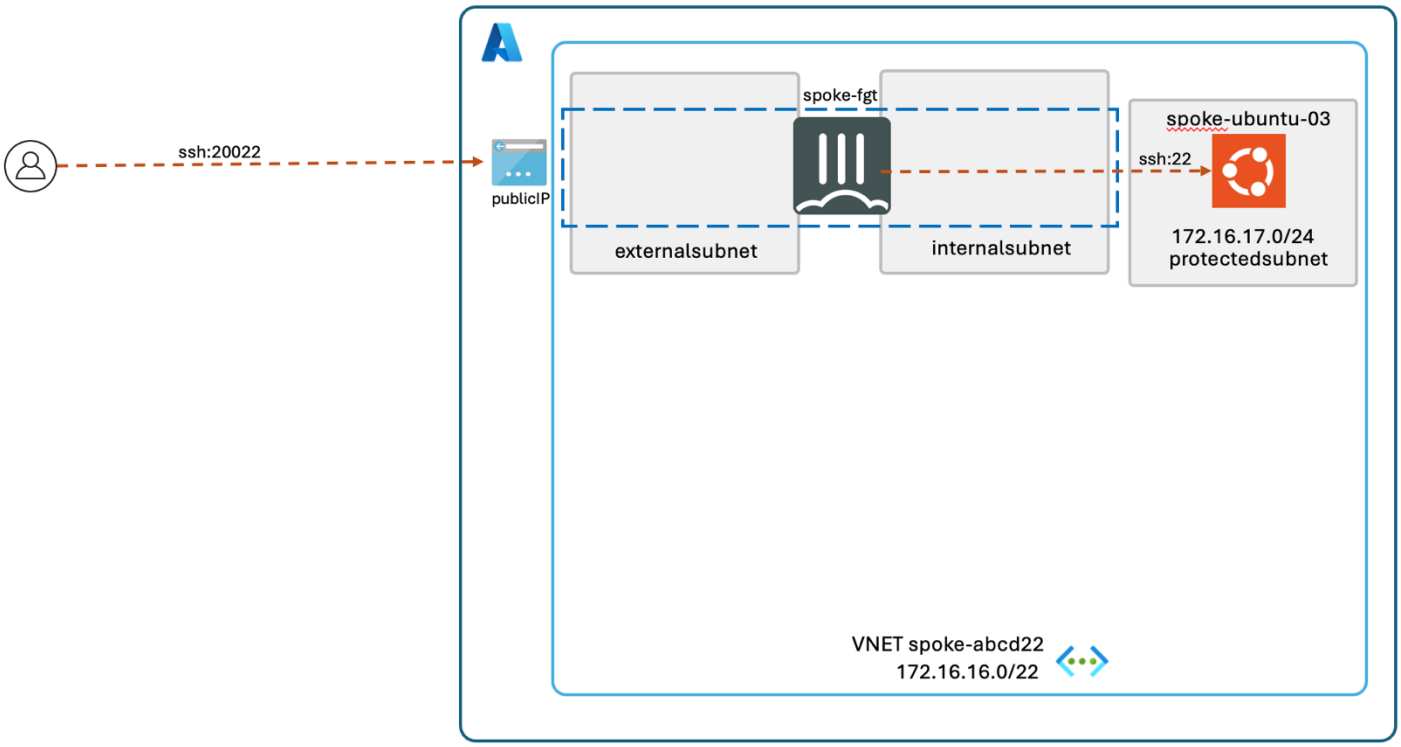
ProtectedSubnet

No Public IP

Review + create

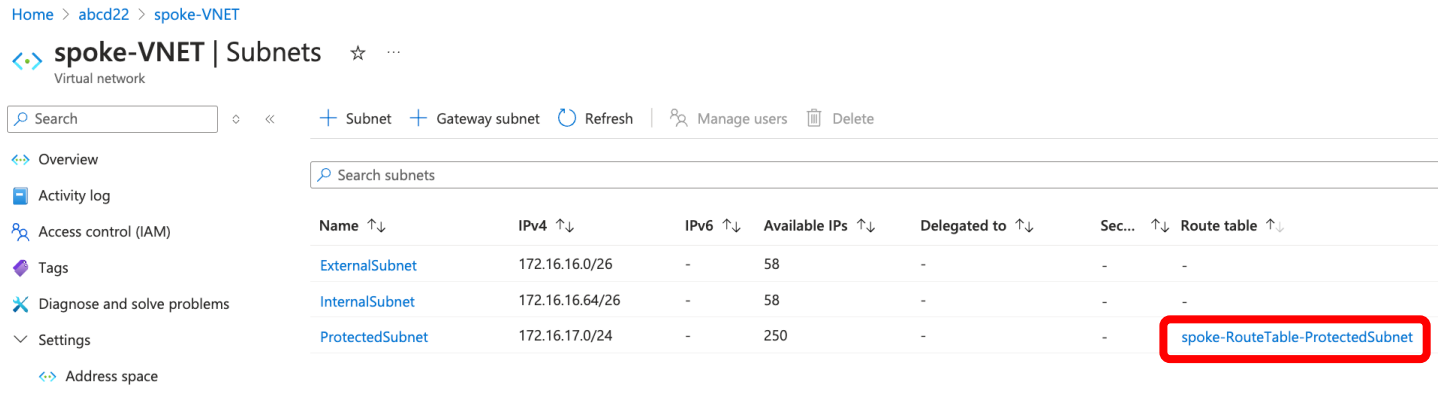
Create

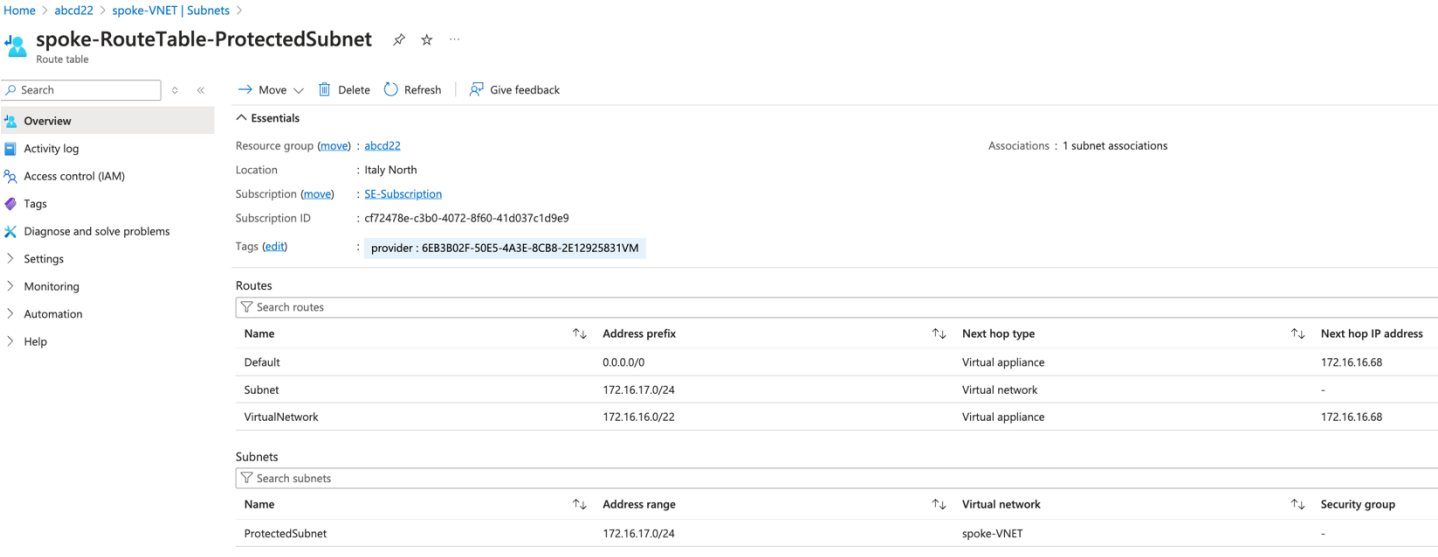
8. SPOKE - Accesso server Ubuntu03 tramite VIP Fortigate spoke



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

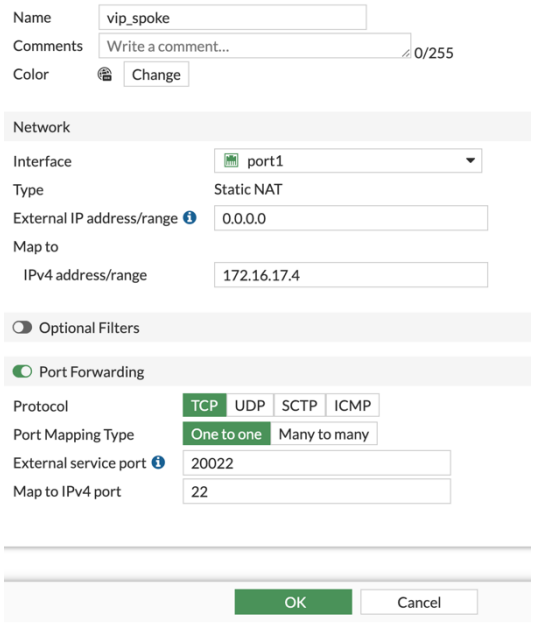
La subnet ProtectedSubnet ha associata una routing table che imposta il default gateway verso l'interfaccia internet del fortigate,





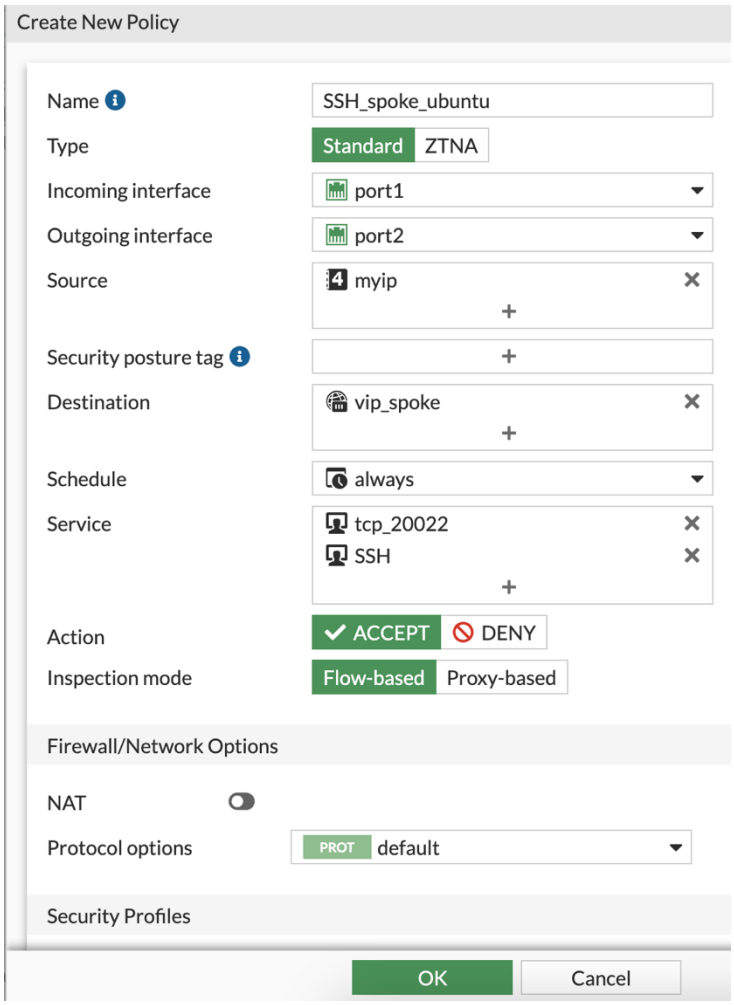
Non occorrerà quindi attivare il NAT nella policy per il flusso in ingress.

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.



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).



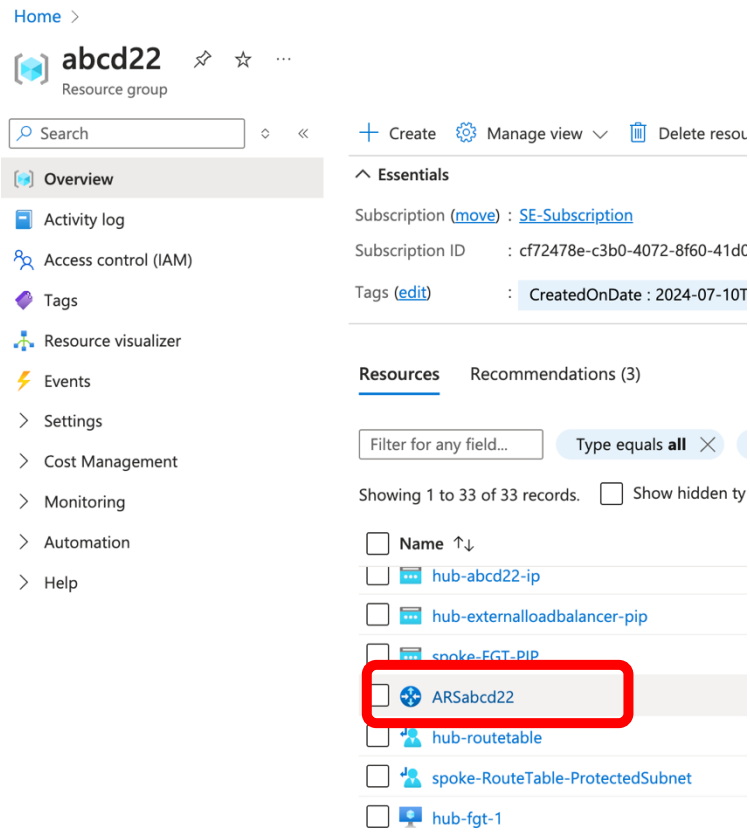
Creare come fatto sul cluster il servizio tcp_20022 e l'oggetto MyIP e infine la policy.

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

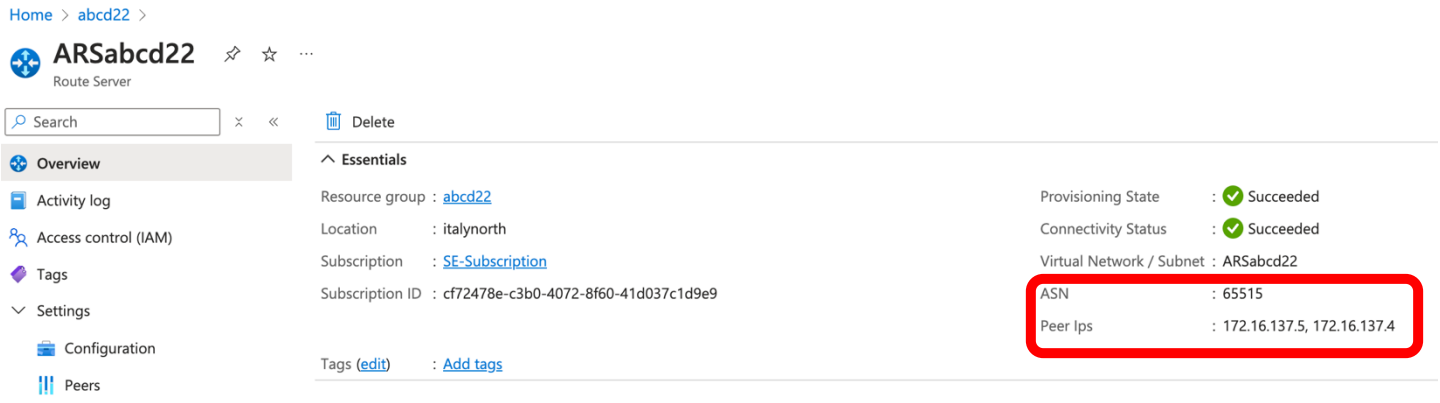
```
ssh abcd22@y.y.y.y –p20022
```

9. Configurazione BGP all'interno della vnet HUB

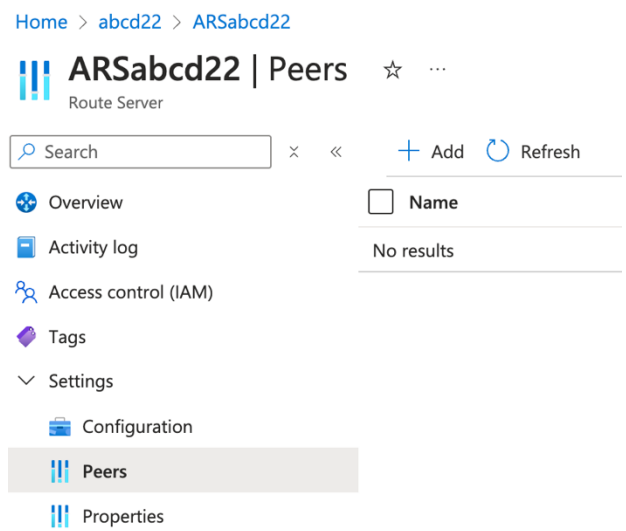
All'inizio del laboratorio è stato creato L'Azure Route Server. Procedere ora alla configurazione del BGP.



Dalla lista delle risorse all'interno del proprio Resource Group click su **ARS<resource group name>**



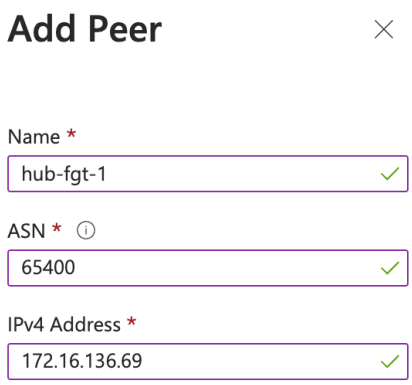
(L'ASN e i due ip del ASR verranno utilizzati più avanti per configurare i neighbor sui fortigate hub)

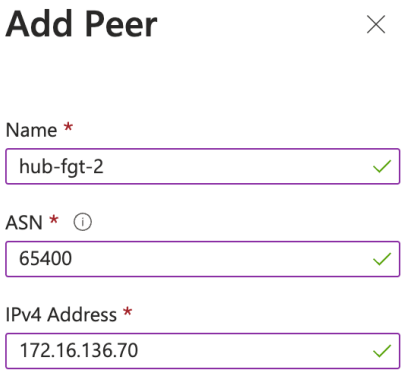


Nel menu a sinistra del Route Server selzionare

Settings -> Peers

Nel menu in alto selezionare ***ADD***





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
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	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

TEST

Da cli verificare il routing

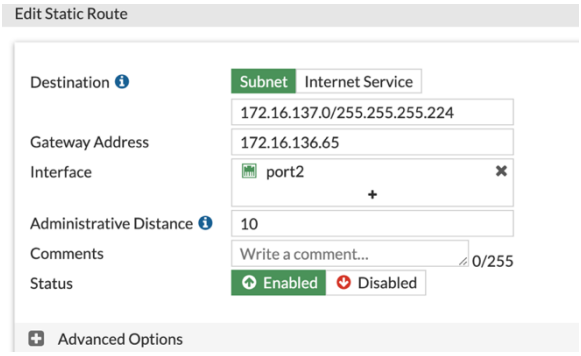
```
get router info bgp summary
get router info bgp network
get router info routing-table all
```

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

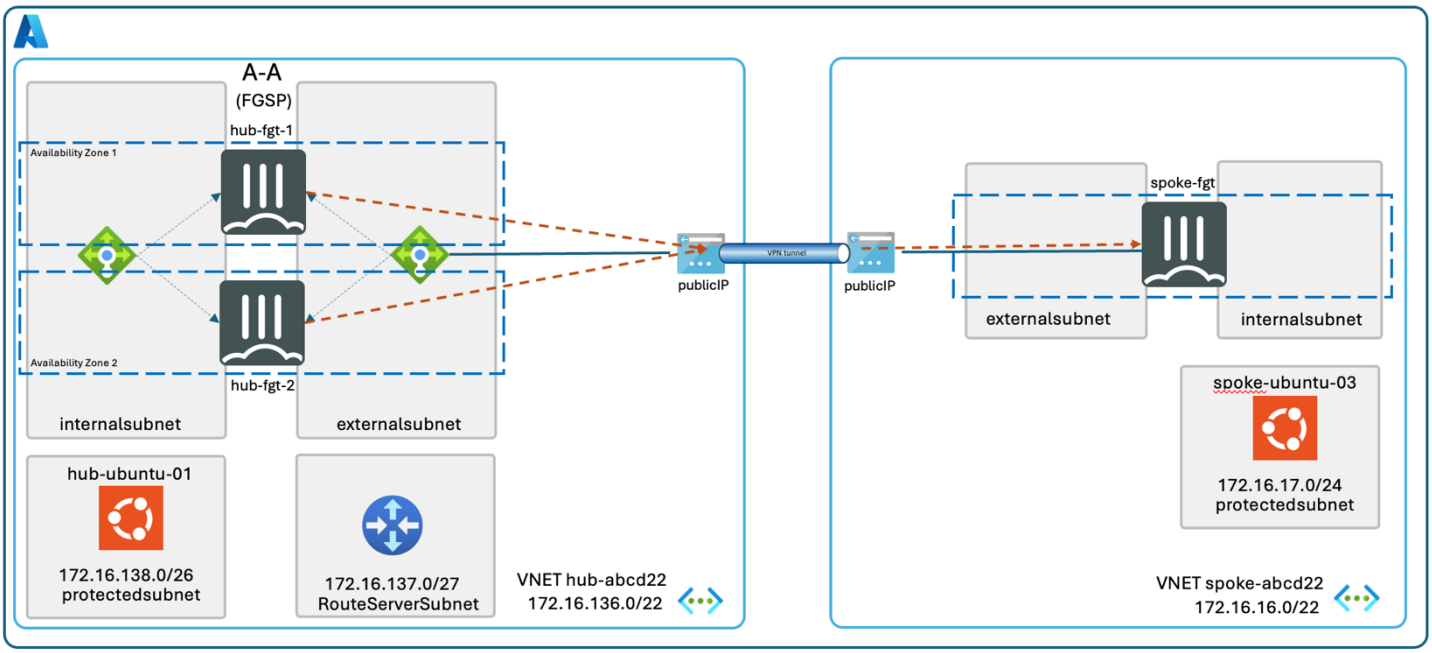
E’ possibile modificare la statica per la 172.16.136.0/22 e sostituirla con la 172.16.137.0/27 per indirizzare ricorsivamente tutta la network della vnet



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

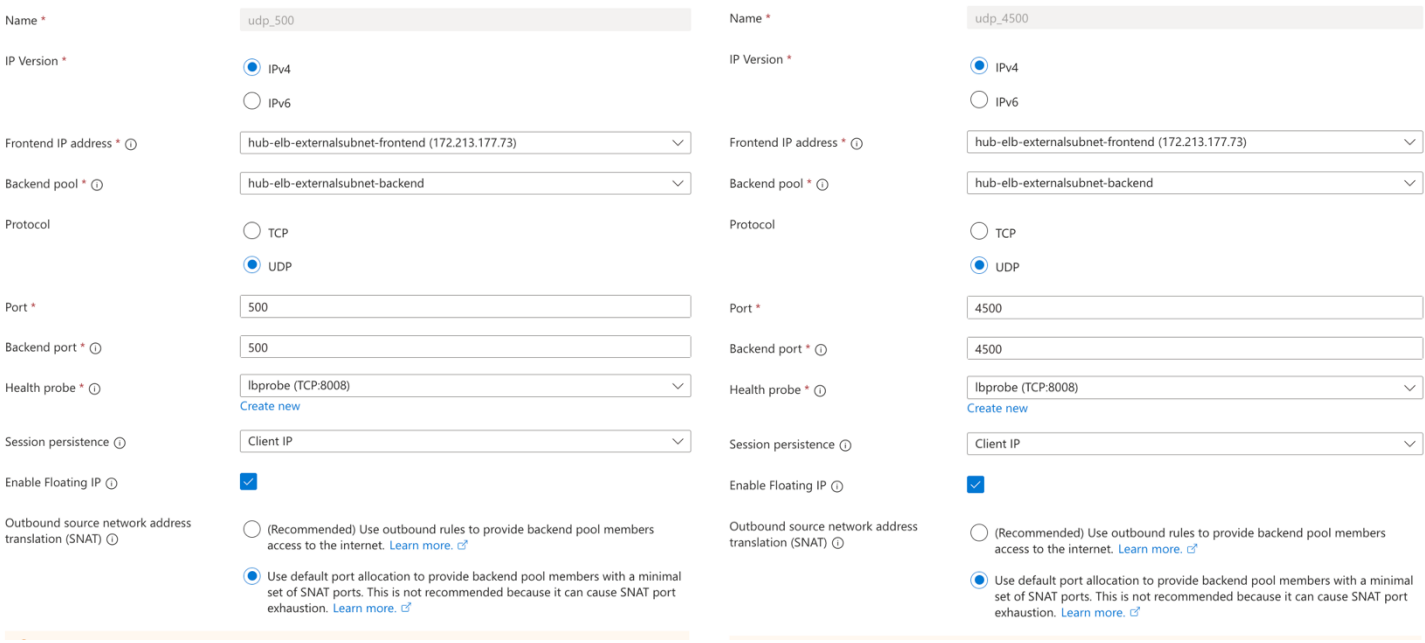
L'HUB riceverà i tunnel tramite bilanciatore, iniziare a configurare le regole di balancing su

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.



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)

(selezionare powershell)

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

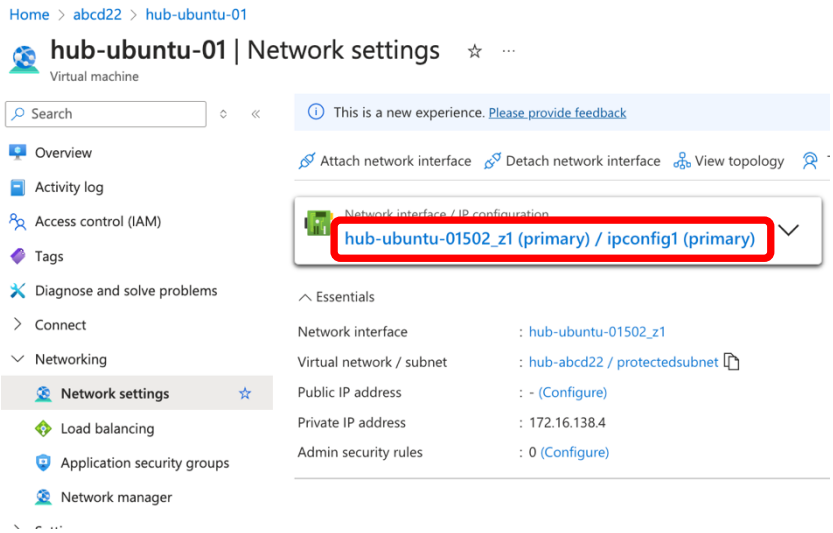
```
Get-AzRouteServerPeerLearnedRoute -ResourceGroupName abcd22 -RouteServerName ARSabcd22 -PeerName hub-fgt-2
```

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

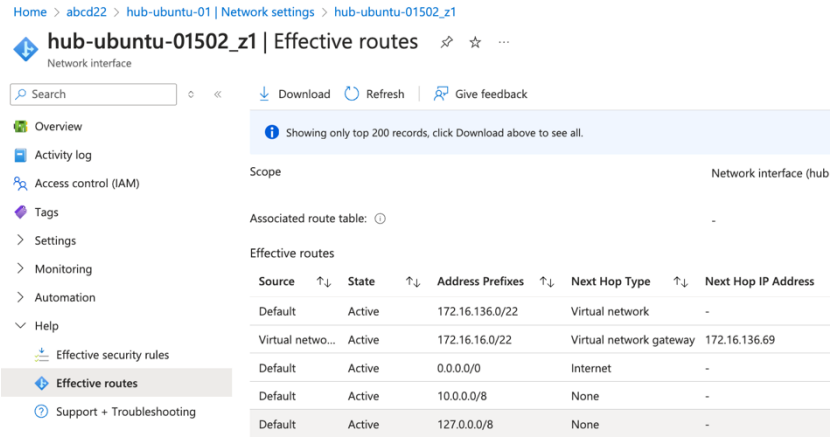
2. *console web Azure.*

In Azure le rotte vengono applicate direttamente alle nic delle vm

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



Selezionare la ***Network Interface***



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

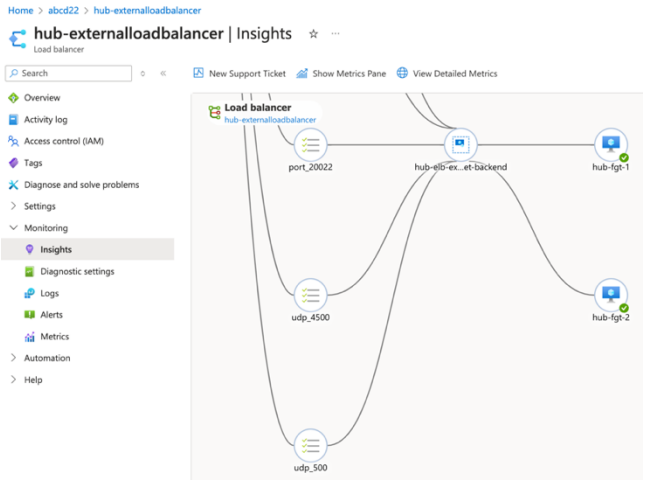
TEST

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***

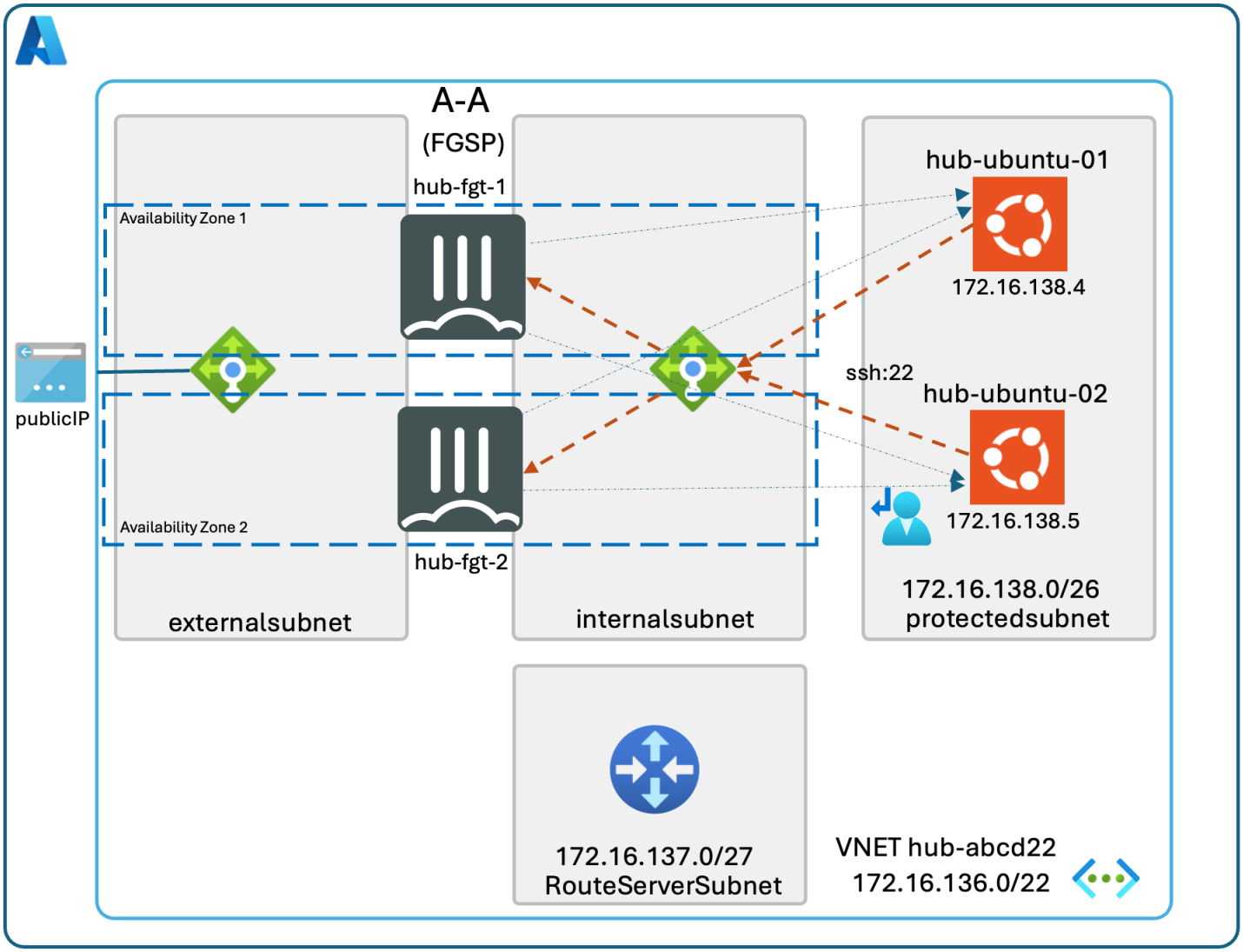
Fare zoom sulle icone dei due nodi fortigate.

Riaccendere il nodo fortigate hub precedentemente spento.

La vpn dopo circa un minuto si risposta sul nodo che è stato riacceso, 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:

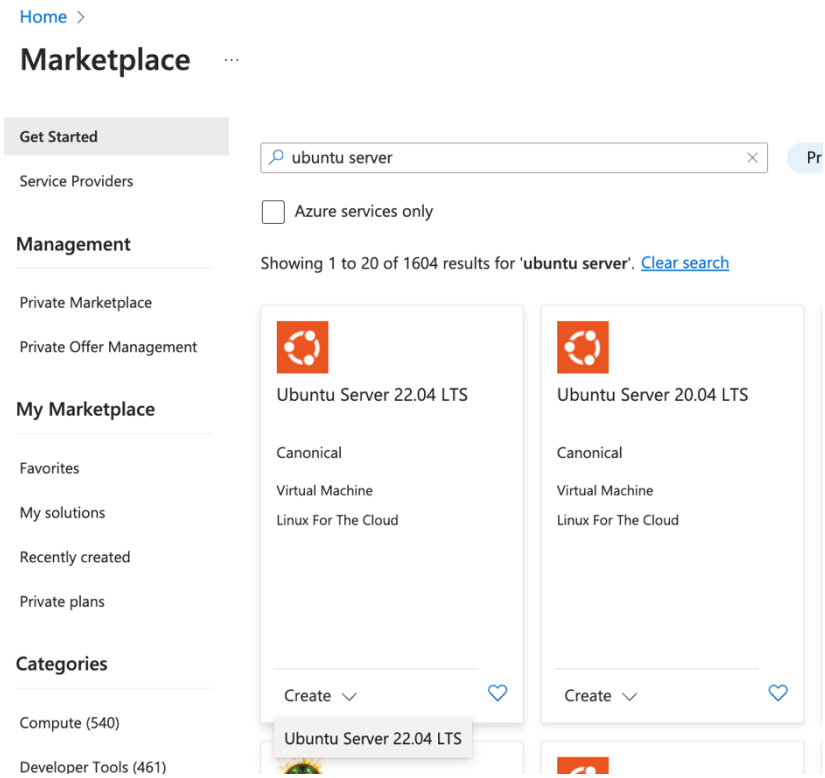
- installazione del server hub-ubuntu-02 nella Protected Subnet
- copnfigurazione nuova routing table da associare alla Protected Subnet
- configurazione policy sui due nodi hub-fgt per permettere l'SSH
- test flussi

Installazione di un nuovo server hub-ubuntu-02

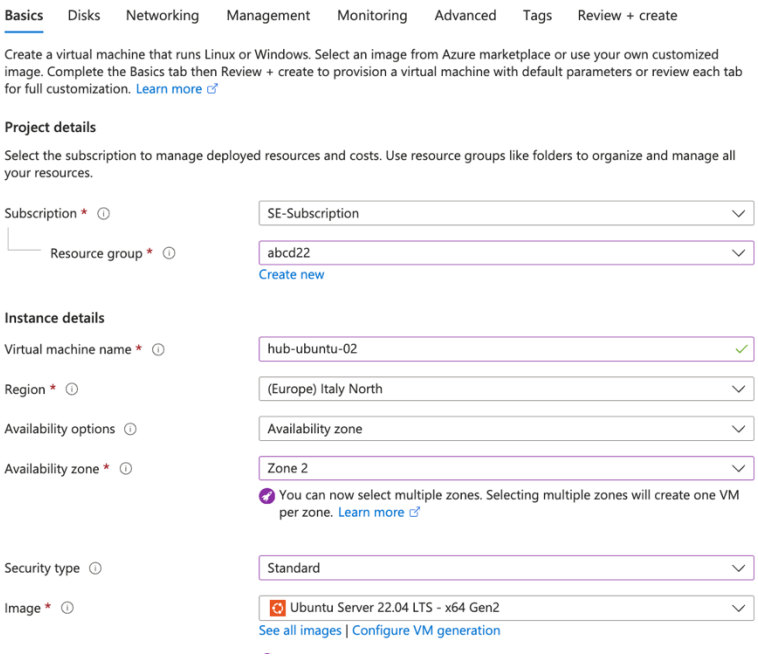
Tornare nella Home della console Azure e entrare nel Marketplace.

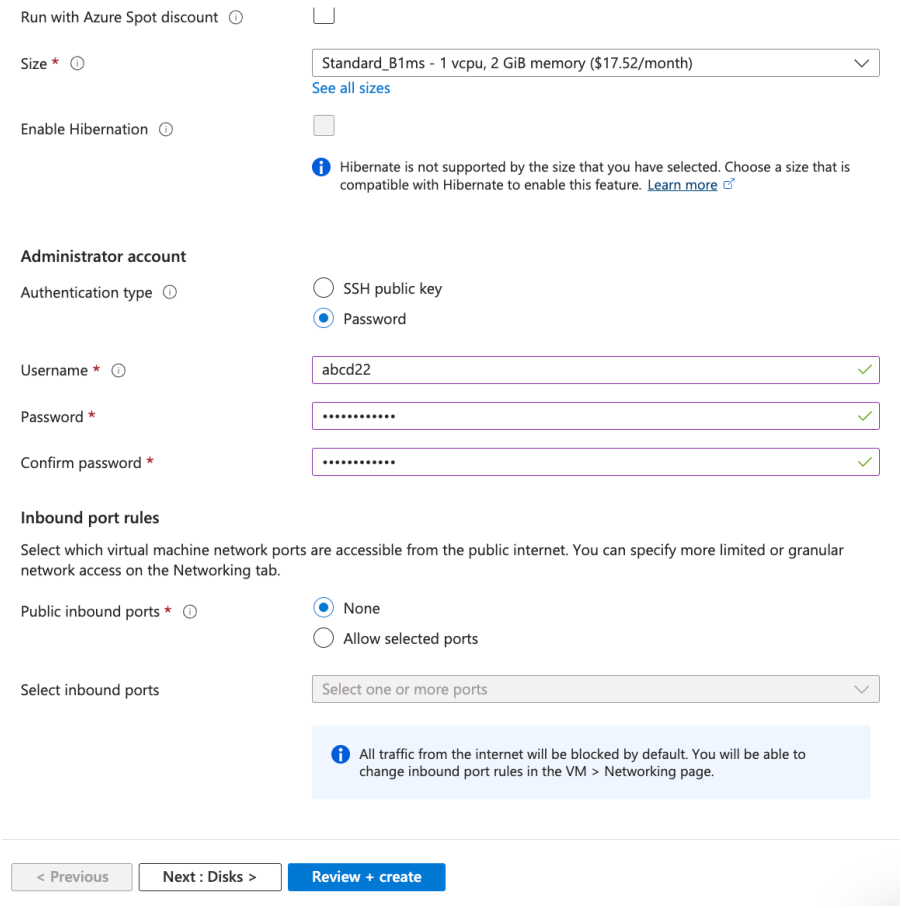
Nel campo search digitare ***ubuntu server*** e dare invio

Selezionare ***Ubuntu Server 22.04 -> Create***



Compilare i parametri come da figura



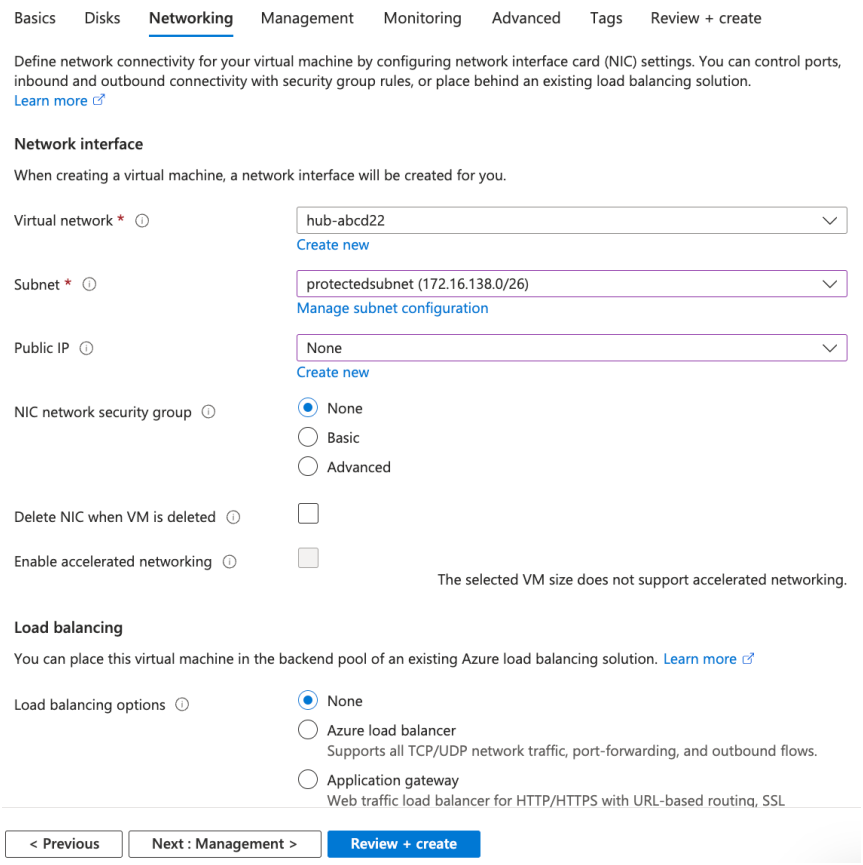


Impostare password

No inbound ports

NEXT

Lasciare le impostazioni di default nella sezione Disk - NEXT



Networking

Compilare i parametri di rete come da figura

Selezionare

La propria HUB-vnet

ProtectedSubnet

No Public IP

Review + create

Create

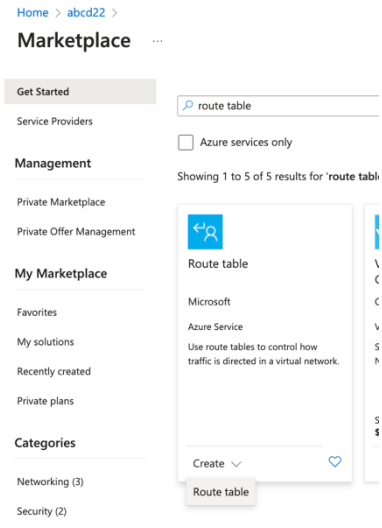
Al termine del deploy di hub-ubuntu-02 verificarne la raggiungibilità:

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

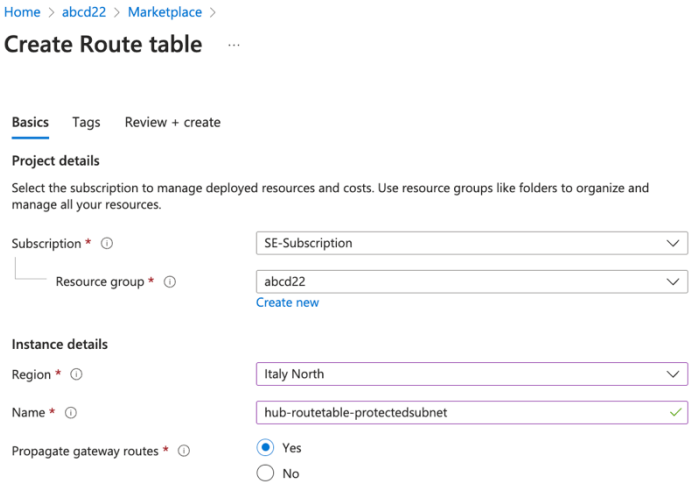
```
ssh abcd22@x.x.x.x –p 20022
ping 172.16.138.5
abcd22@hub-ubuntu-01:~$ ssh abcd22@172.16.138.5
```

Creazione e configurazione nuova routing table

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



Create



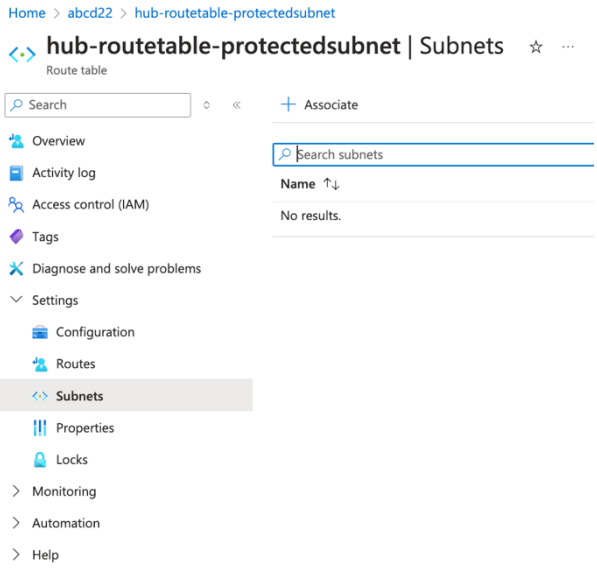
Impostare i parametri come in figura

Lasciare abilitata l'opzione Propagate routes

Review + create

Create

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



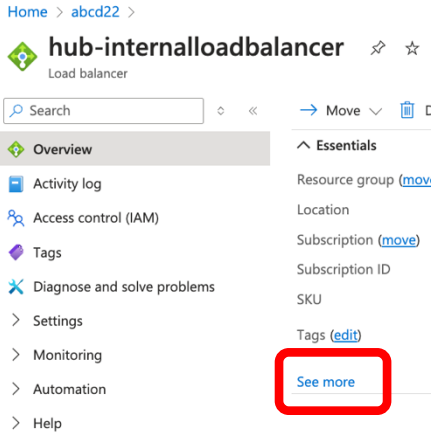
Dal menu a sinistra selezionare **Settings -> Subnet**

Dal menu in alto selezionare ***Associate***

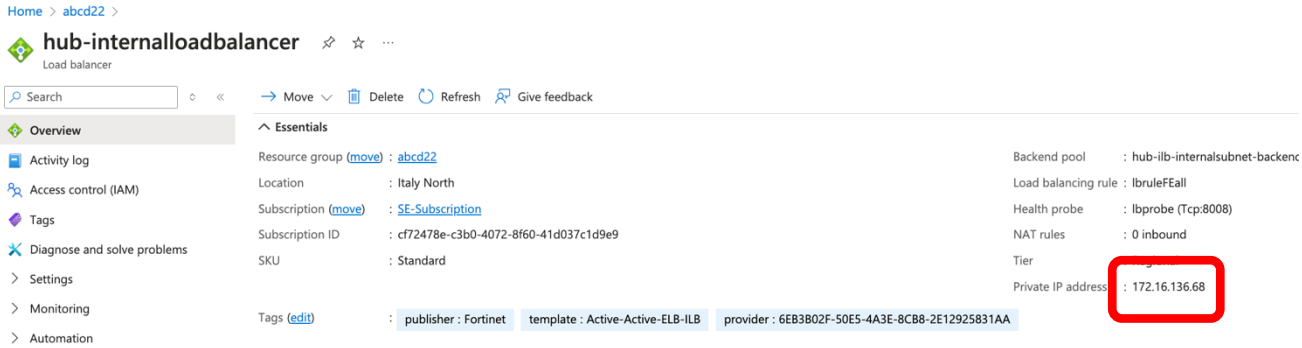
Selezionare la propria vnet hub e la protectedsubnet.

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 baalncert selezionare dall'elenco risorse ***hub-internalloadbalancer.***



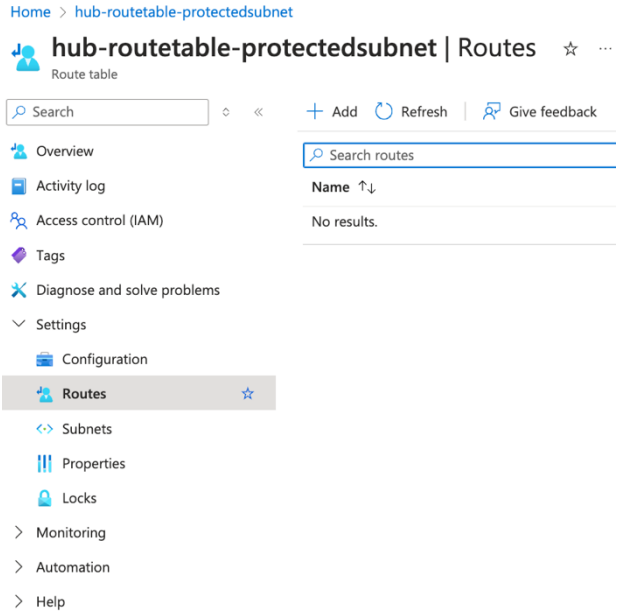
Selezionare ***See more***



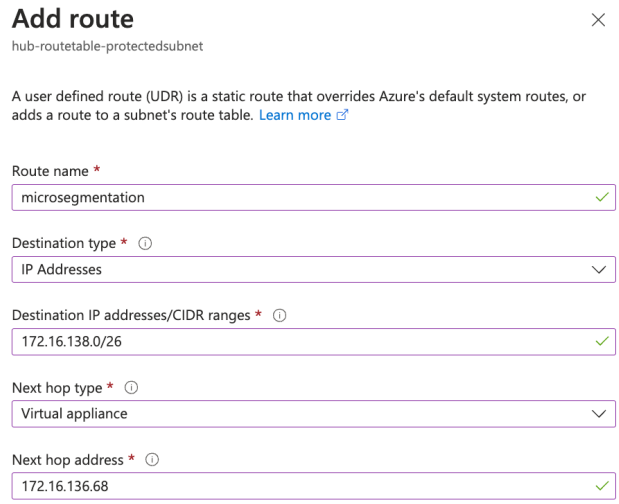
L'ip appare a destra

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

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



Dal menu in alto selezionare ***Add***



Inserire i parametri come in figura.

Add

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

TEST

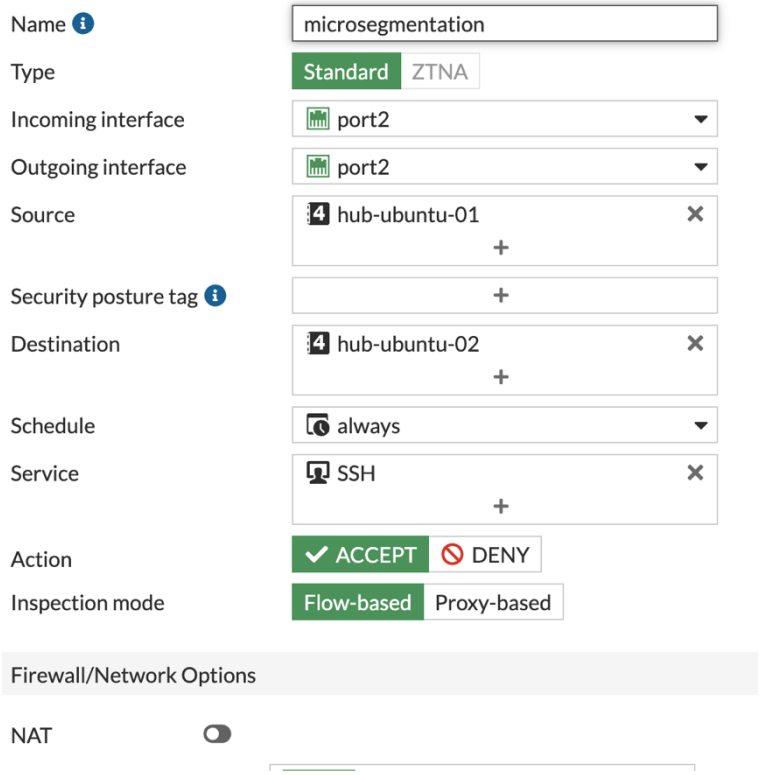
Verificare l'impossibilità della sessione ssh tra hub-ubuntu-01 e hub-ubuntu-02.

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



hub-ubuntu-01: 172.16.138.4

hub-ubuntu-02: 172.16.138.5

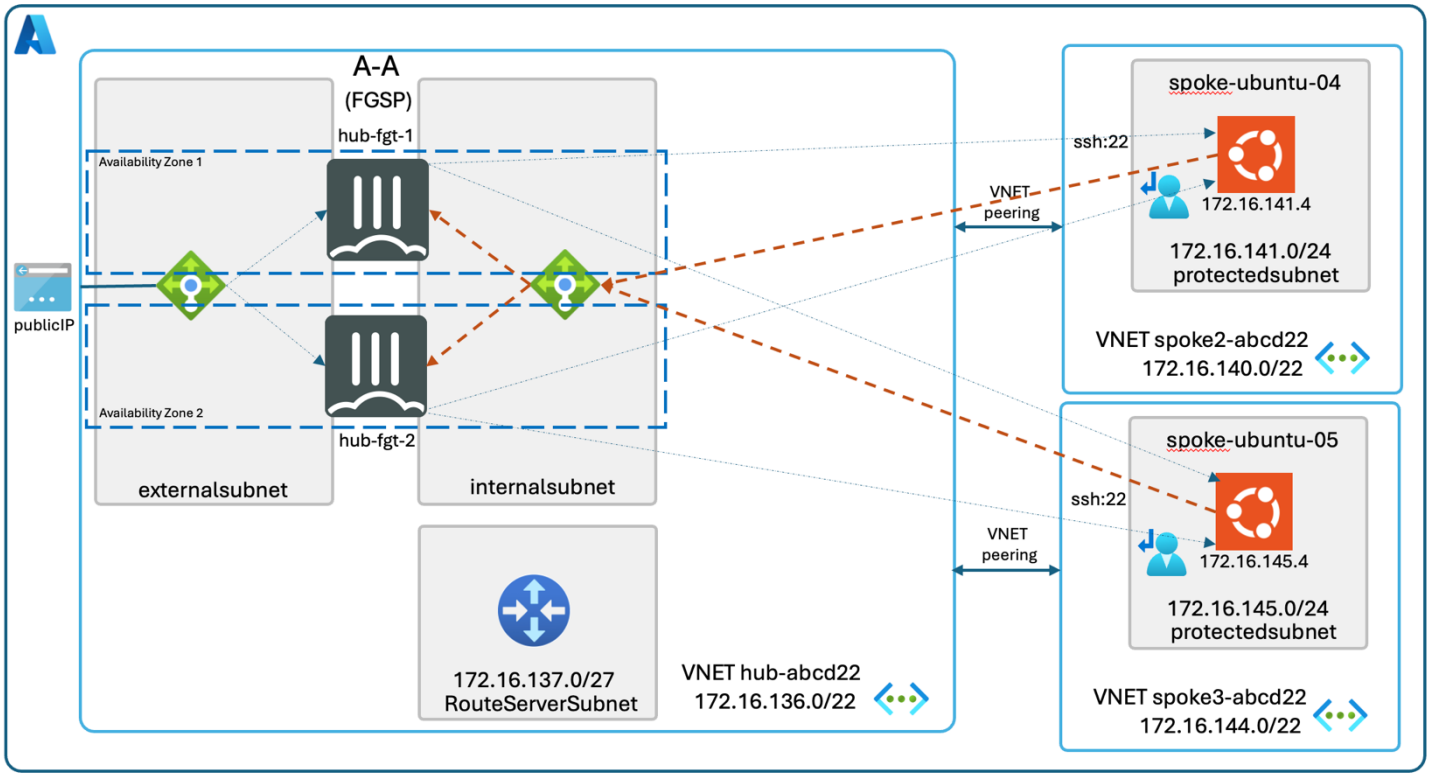
Non è necessario abilitare il NAT poiché le sessioni est-ovest attraversano solo il bilanciatore interno.

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

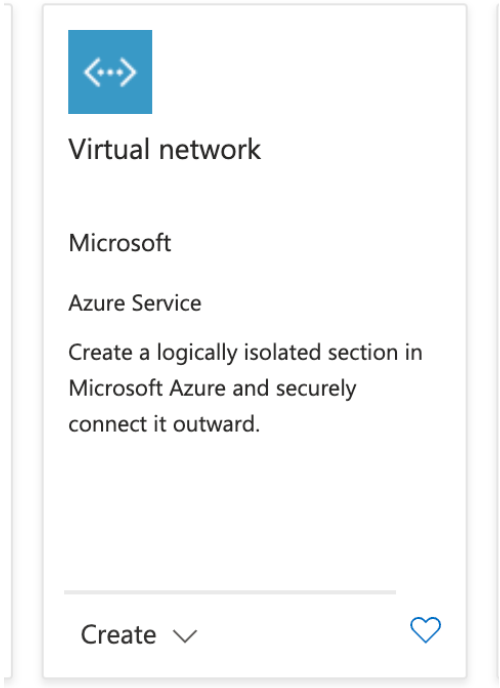
Task dell'esercizio:

- 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

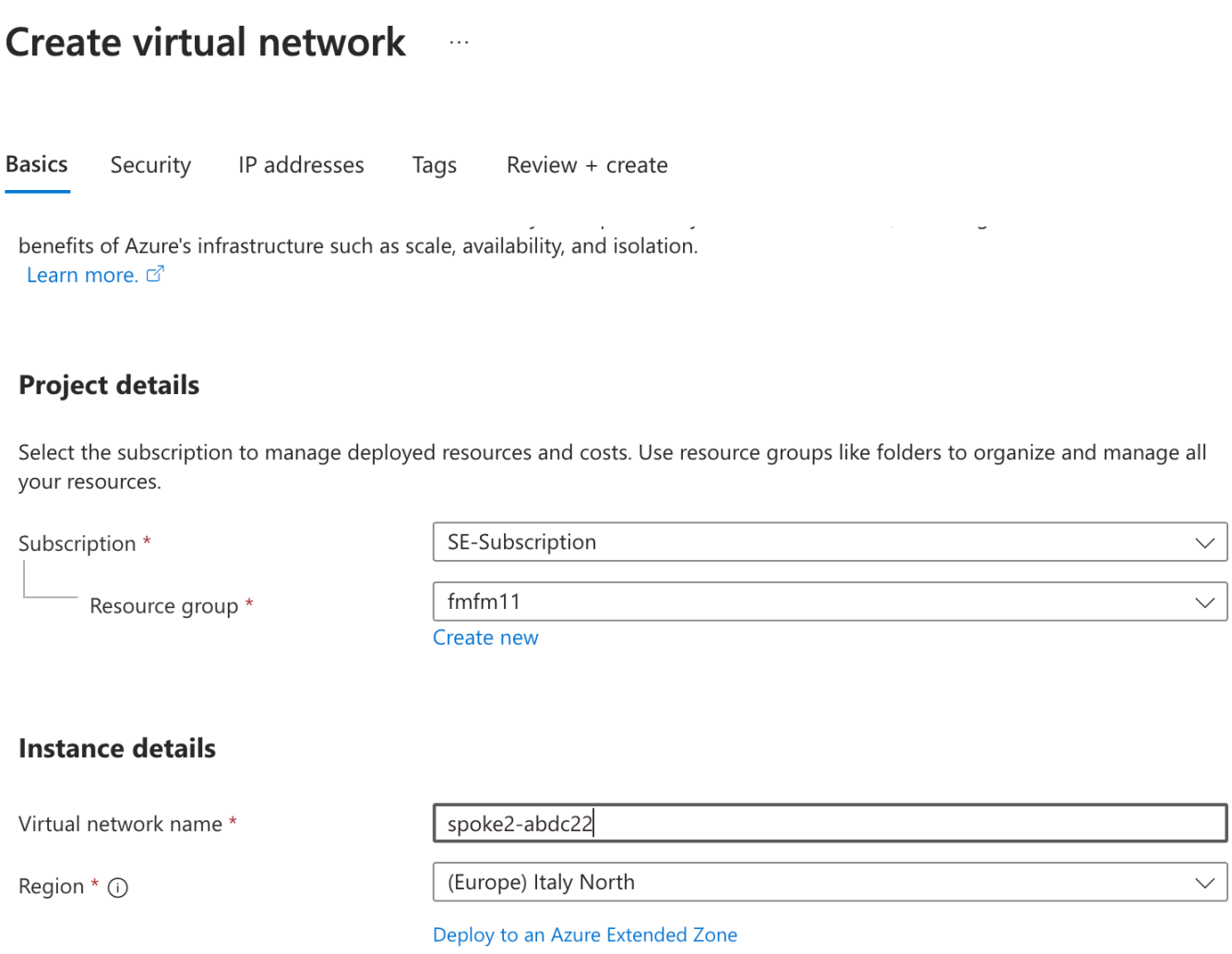
12.1. Creazione nuova VNET son una subnet Protected

Dal MarketPlace cercare Virtual Network.

Selezionare Virtual Network e fare "Create > Virtual Network"

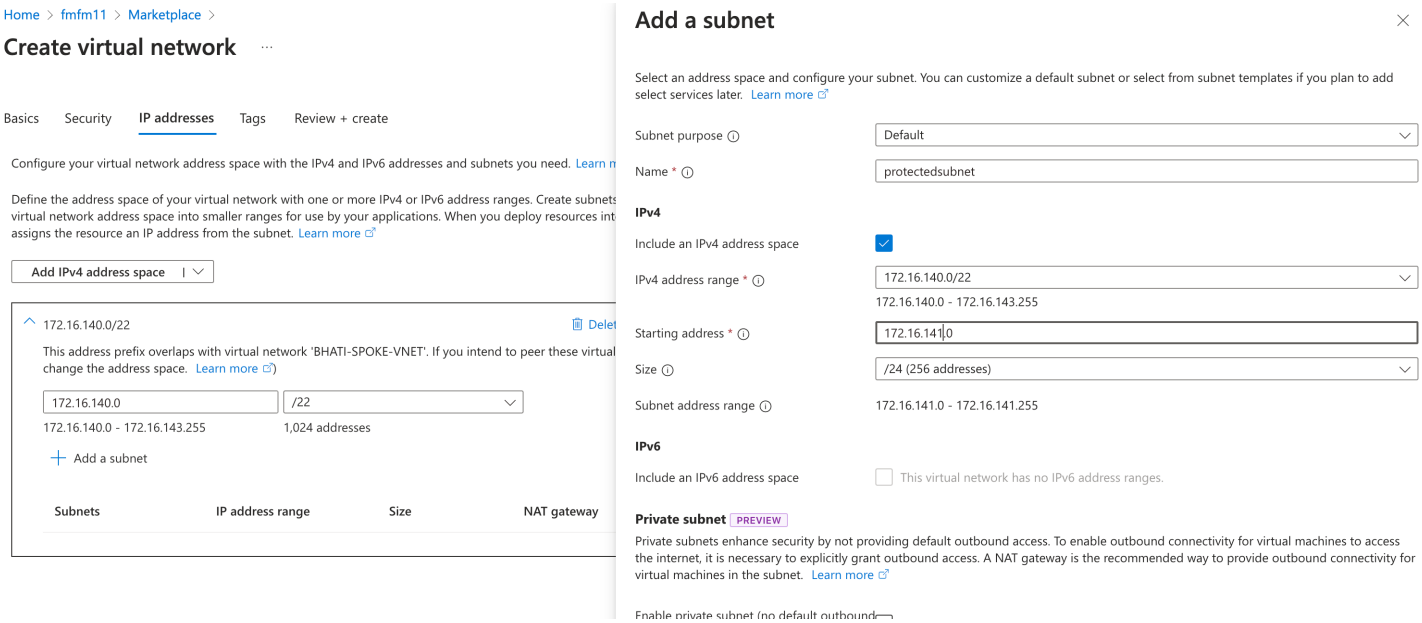


Scegliere il proprio Resource Group e nominare la VNET come spoke2-<nome resource group>



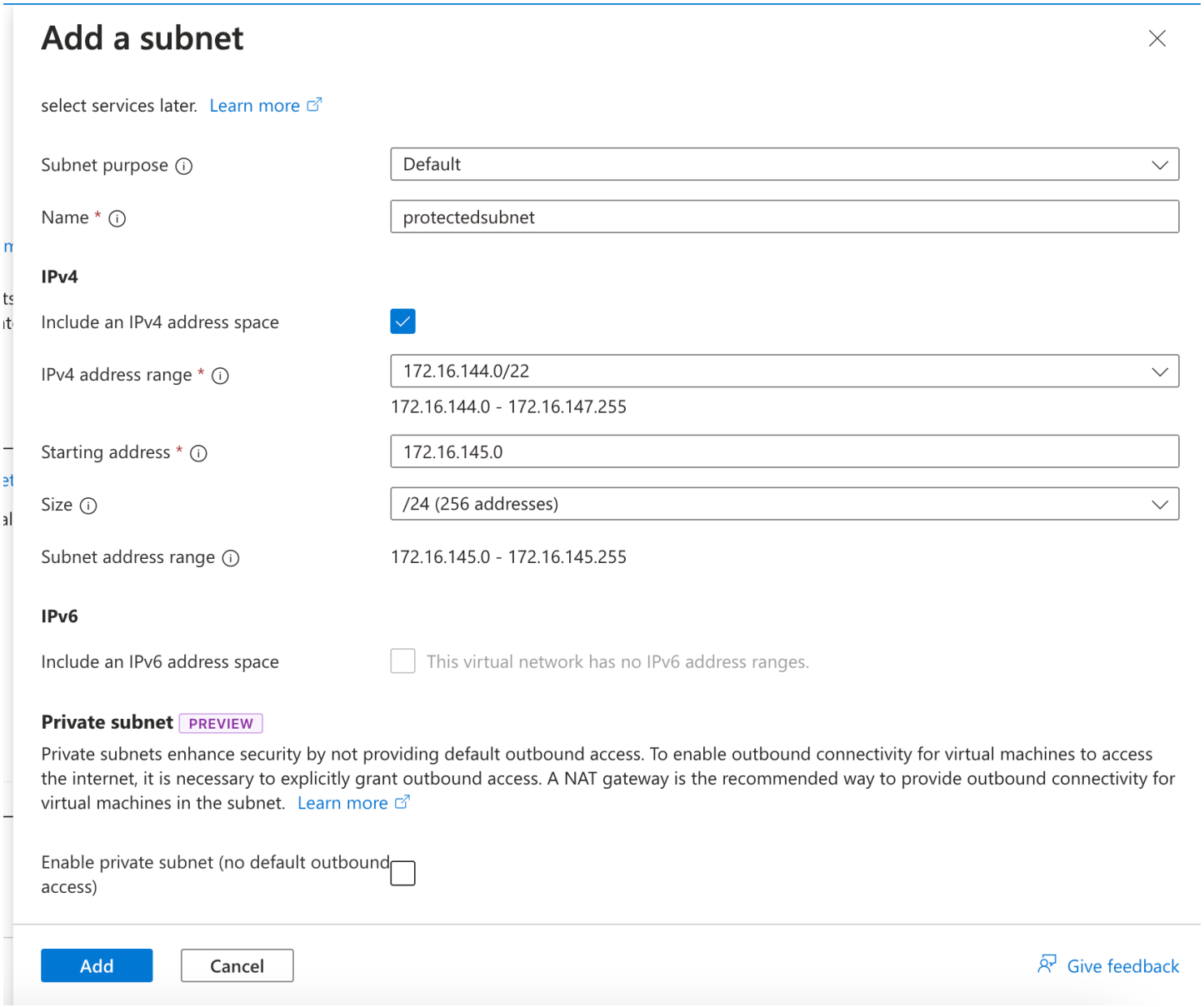
Next, Next fino a "IP addresses"

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



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:



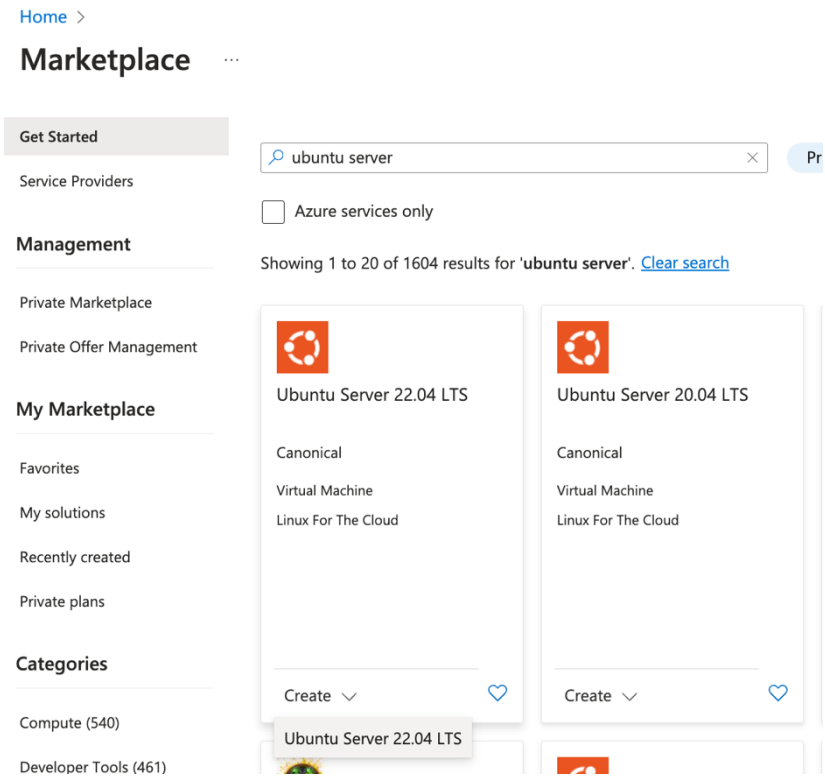
12.2. Creazione nuove VM all'interno delle nuove VNET

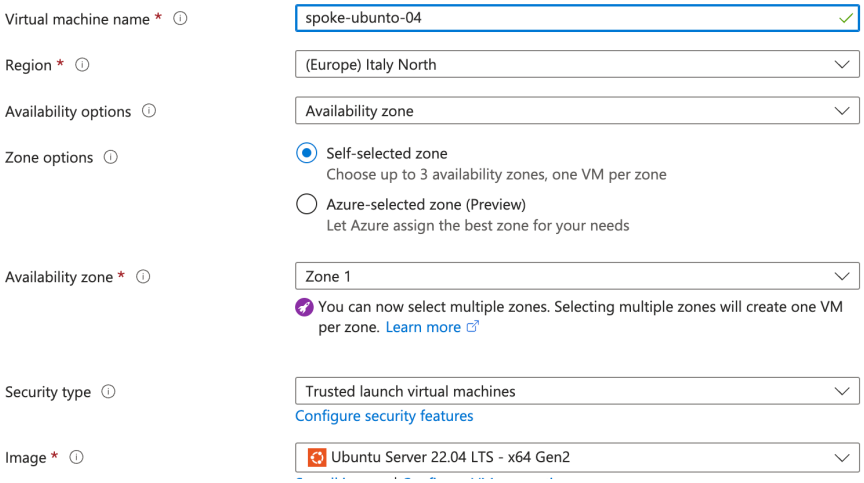
Installare un nuovo server spoke-ubuntu-04.

Tornare nella Home della console AZURE e entrare nel Marketplace.

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

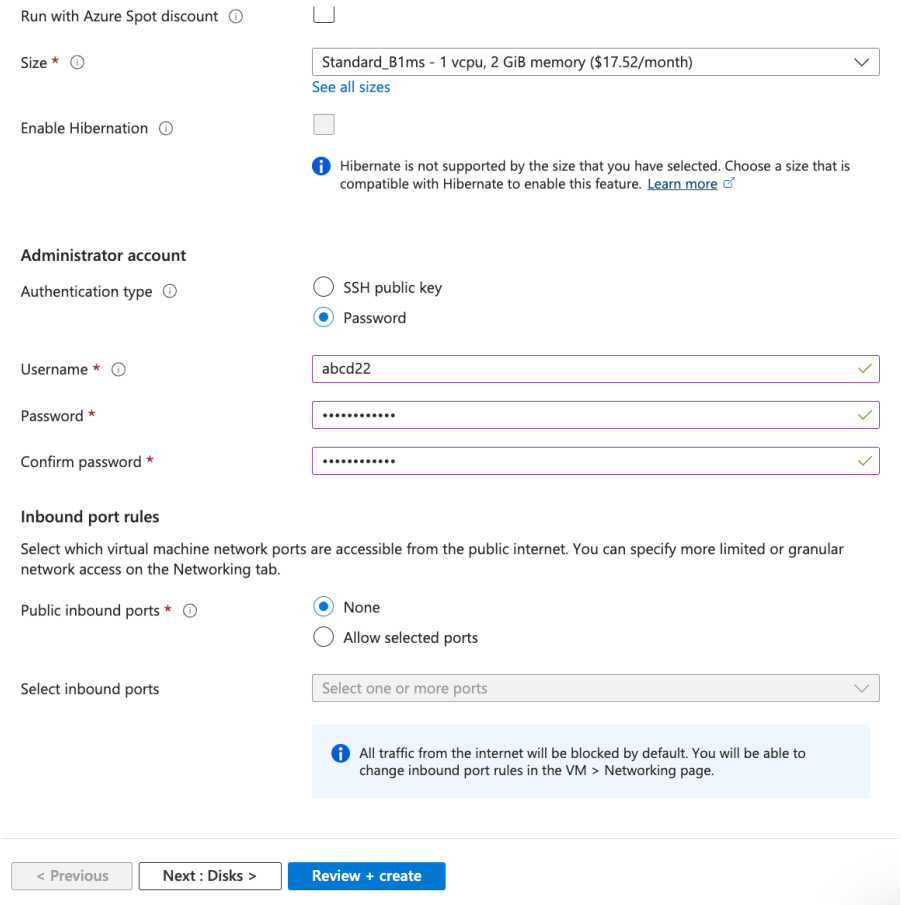
Selezionare ***Ubuntu Server 22.04 -> Create***





Compilare i parametri scorrendo le opzioni fino in fondo

Compilare i parametri come da figura



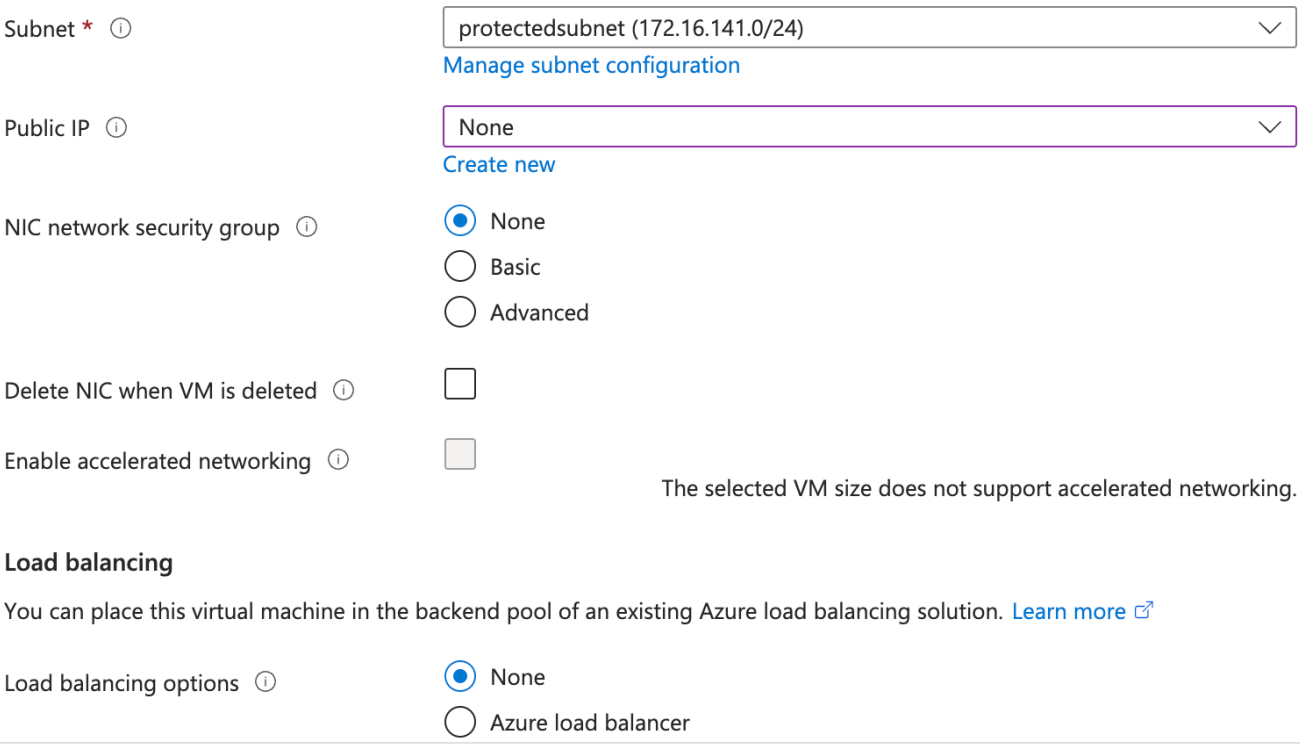
Impostare password

No inbound ports

NEXT

NEXT

Lasciare le impostazioni di default nella sezione Disk - NEXT



Networking

Compilare i parametri di rete come da figura

Selezionare

La nuova spoke-vnet

ProtectedSubnet

No Public IP

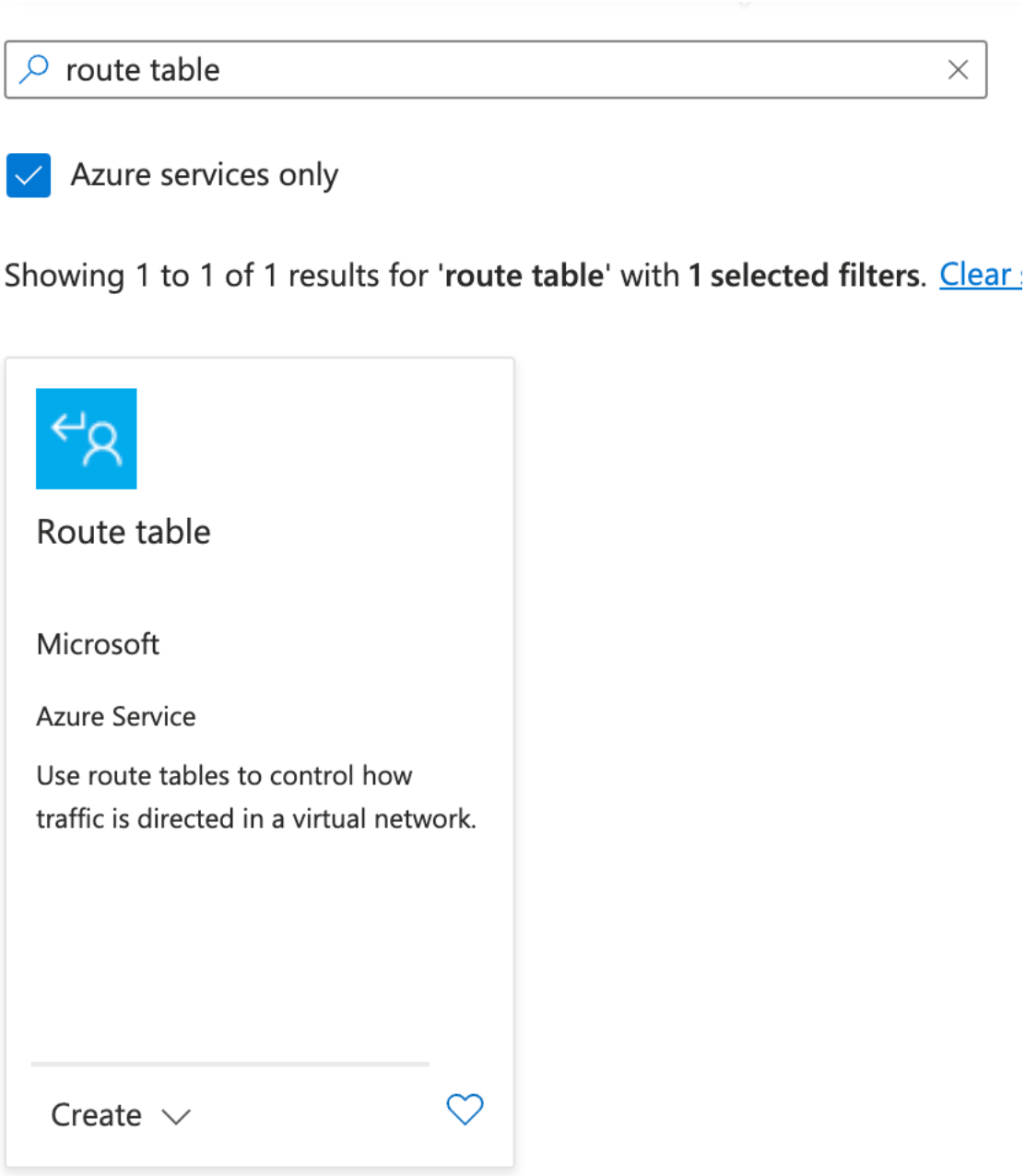
Review + create

Create

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

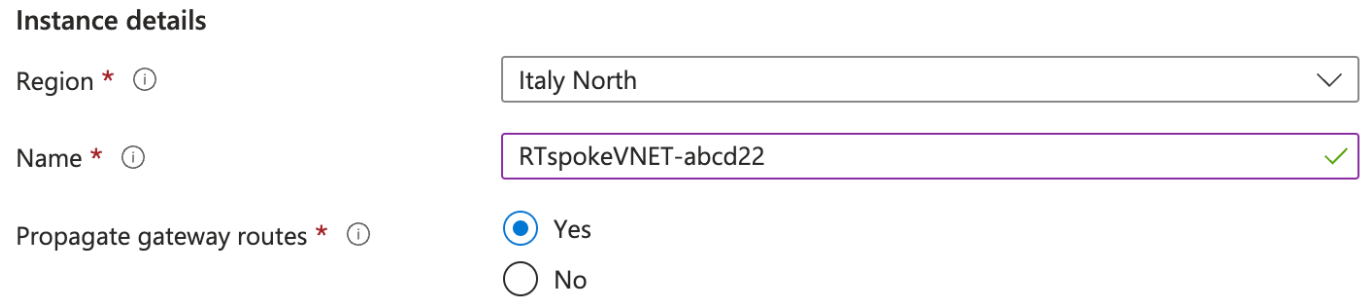
12.3. Creazione nuova Route Table da associare alle nuove Subnet

Su MarketPlace cercare Route Table



Create Route Table

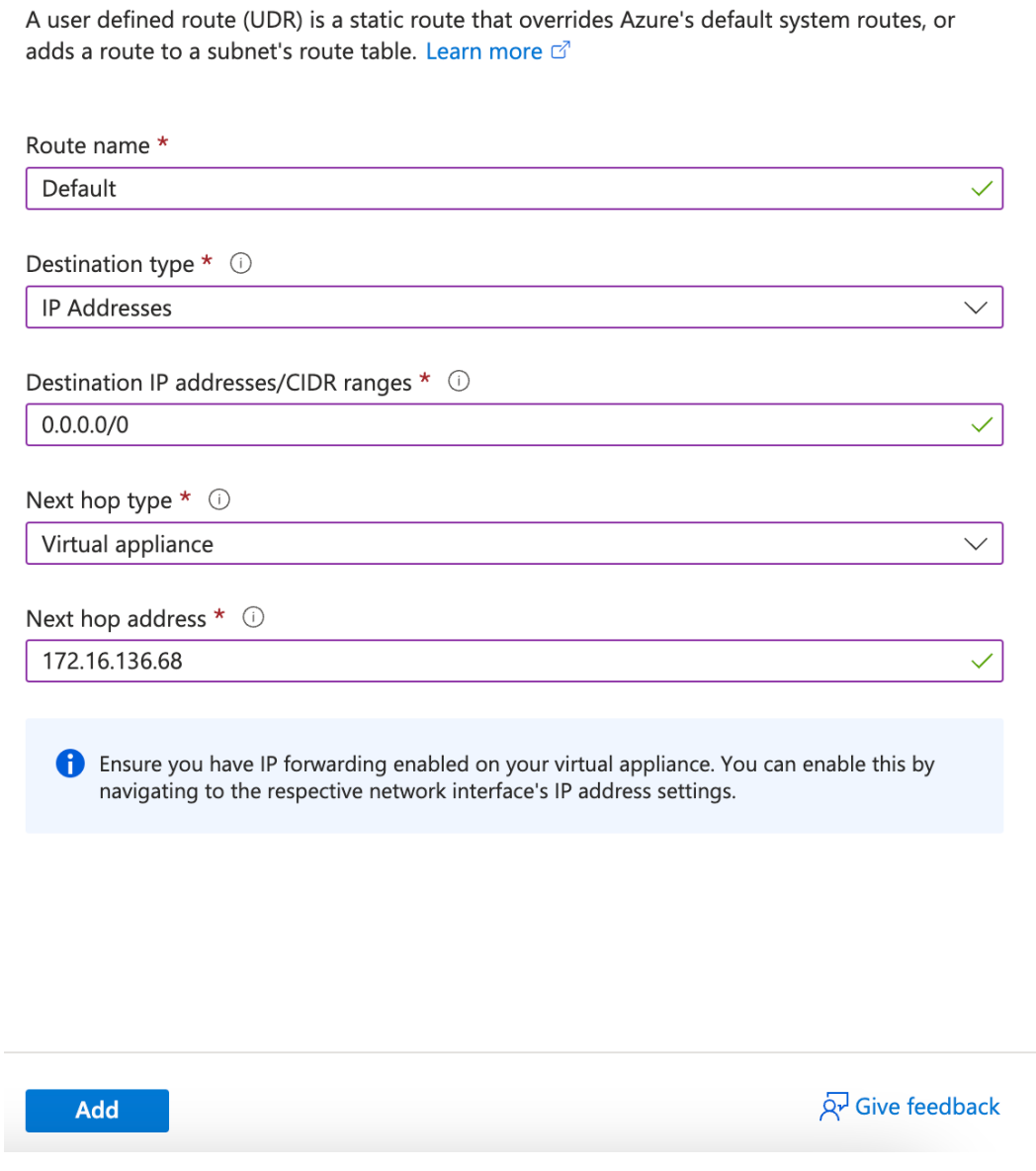
Dare il nome RTspokeVNET-<nomeRG>



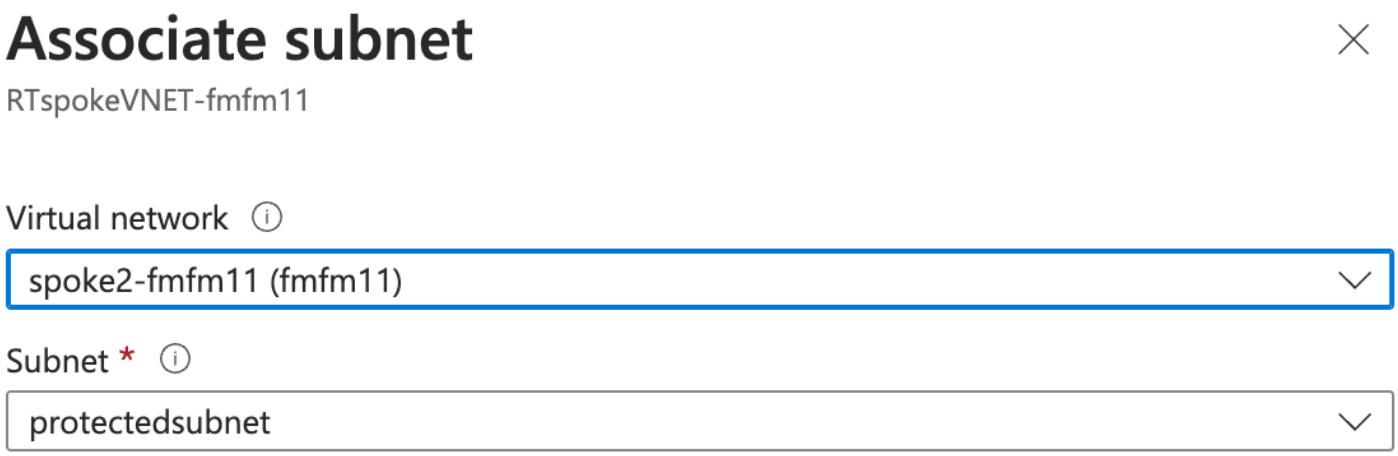
Review and Create, Create

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:



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



Fare OK

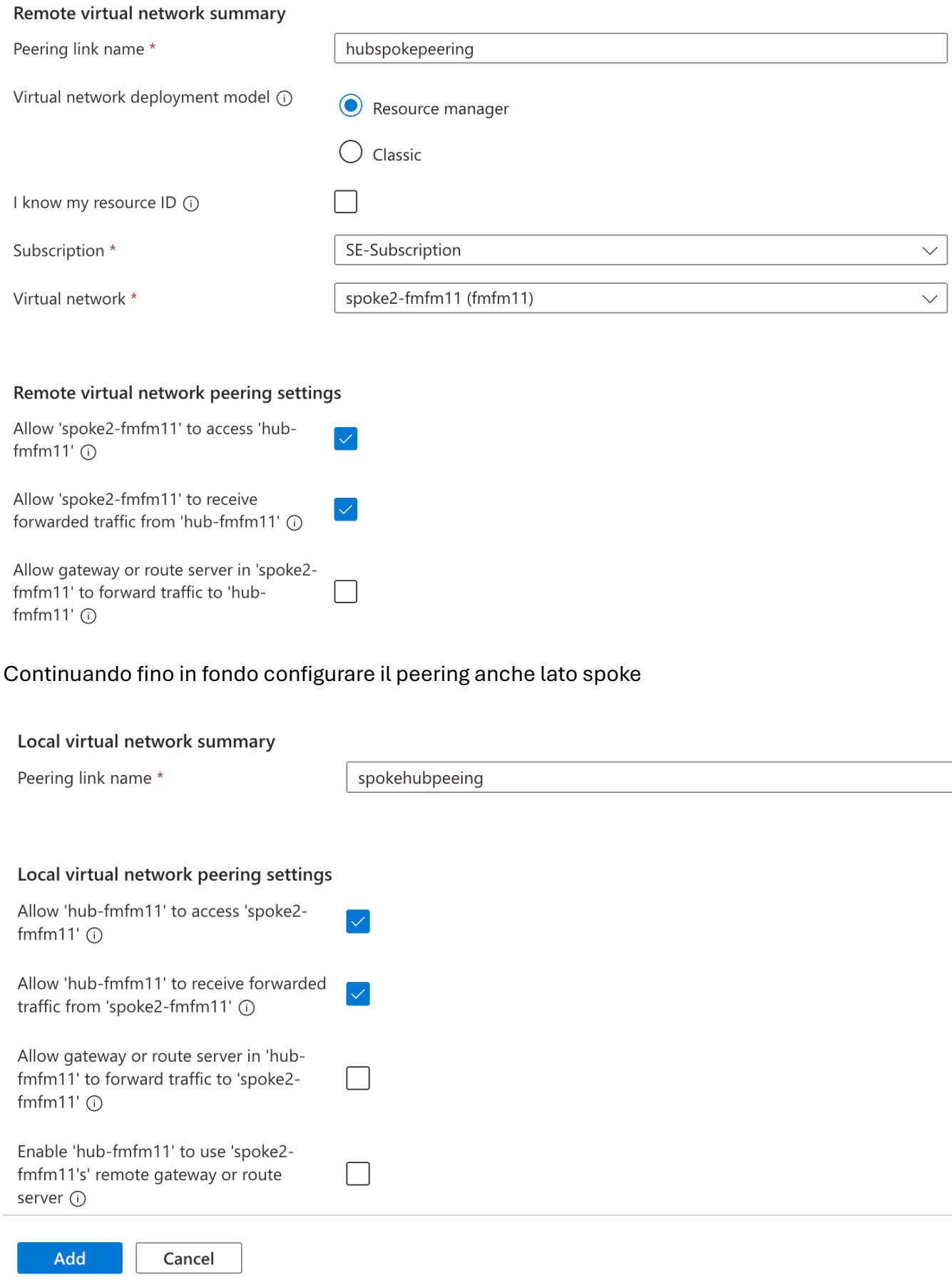
12.4. Configurazione VNET Peering

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



Continuando fino in fondo configurare il peering anche lato spoke

Fare Add

Ripetere per la VNET Spoke3.

12.5. Impostare il routing sui due Fortigate HUB

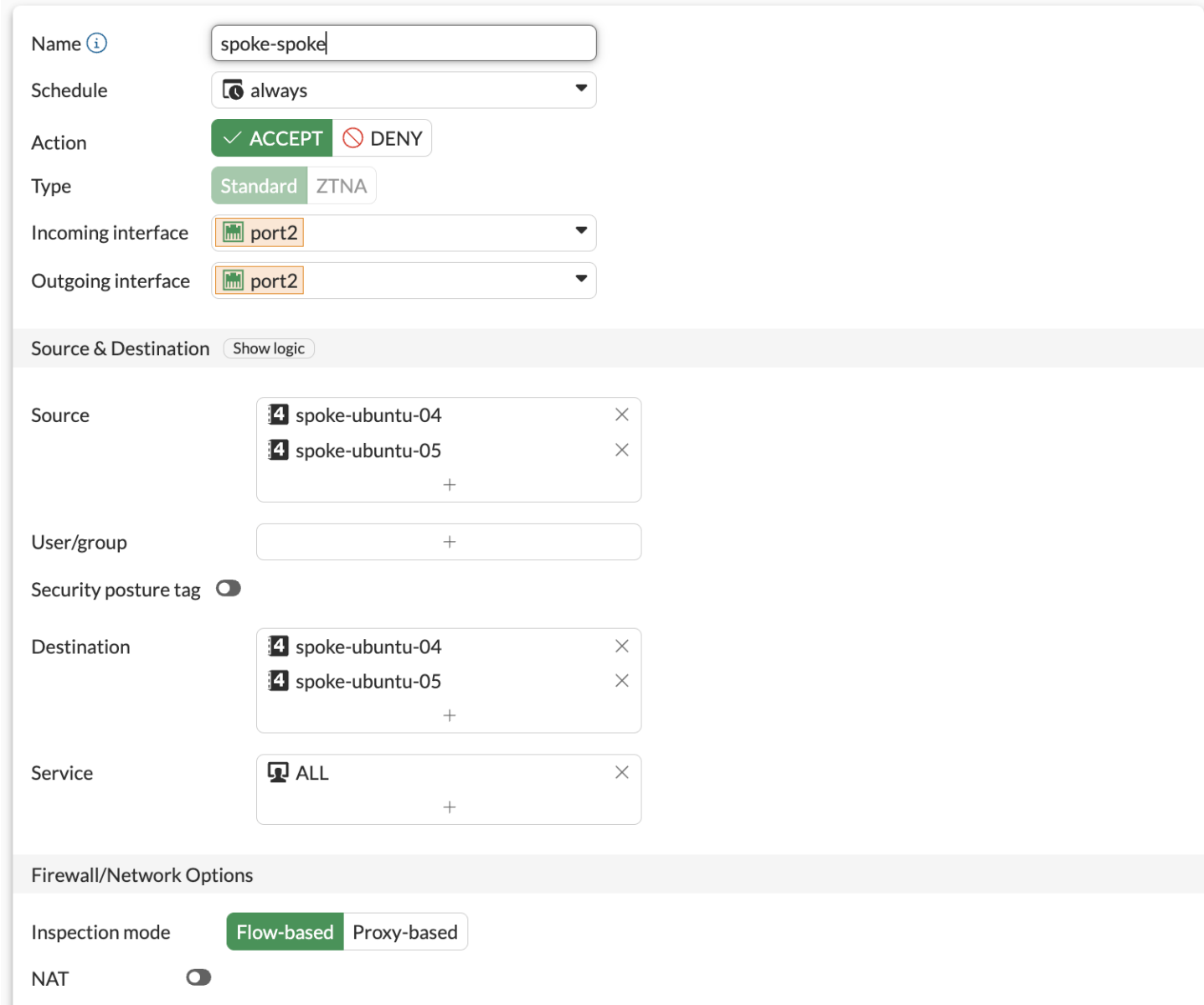
Il next Hop verso le subnet 172.16.141.0/24 e 172.16.145.0/24 dovrà essere il system route interno 172.16.136.65. Impostare le rispettive rotte statiche su entrambi i firewall HUB.

Creare la regola firewall per permetter 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.



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-ubunto-4 fare ping verso spoke-ubuntu-05 (172.16.145.4).

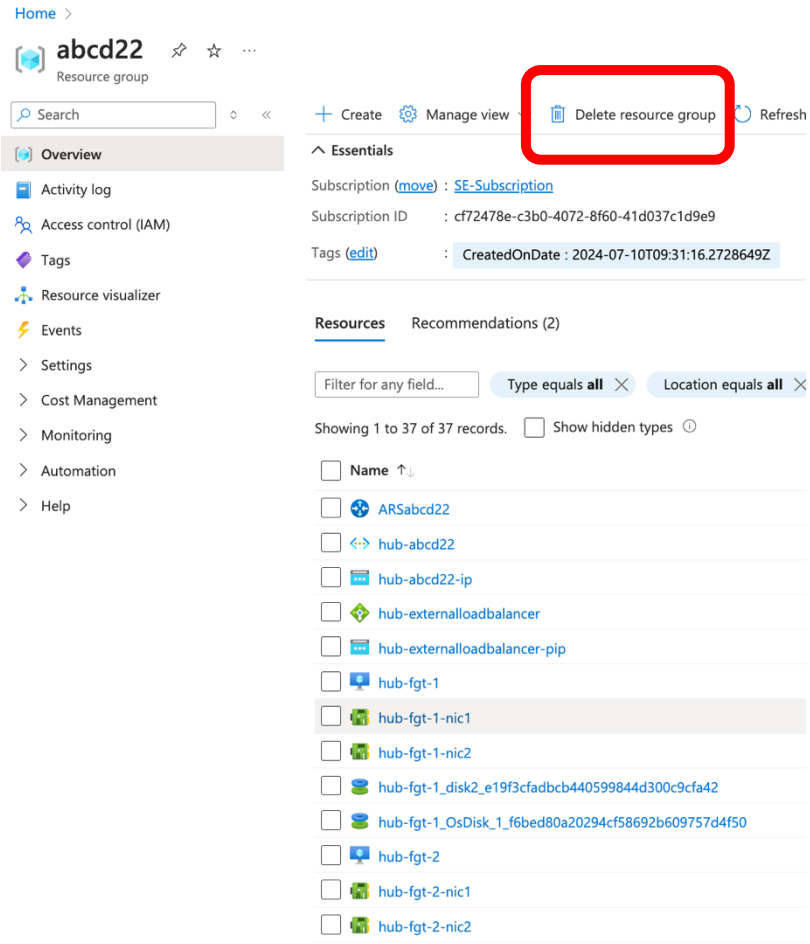
Provare a fare anche SSH da spoke-ubuntu-04 verso spoke-ubuntu-05.

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

13. Rimozione risorse

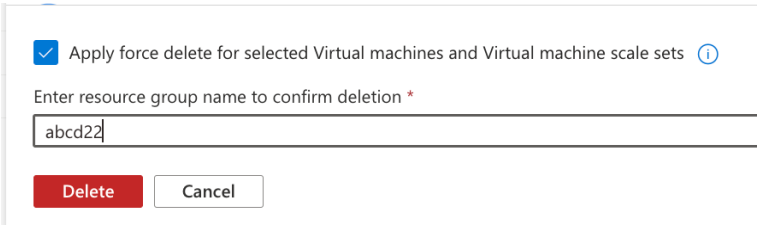
Prima di concludere il LAB rimuovere tutte le risorse create.

Dalla home selezionare il proprio resource group



nel menu in alto selezionare

Delete resource group



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