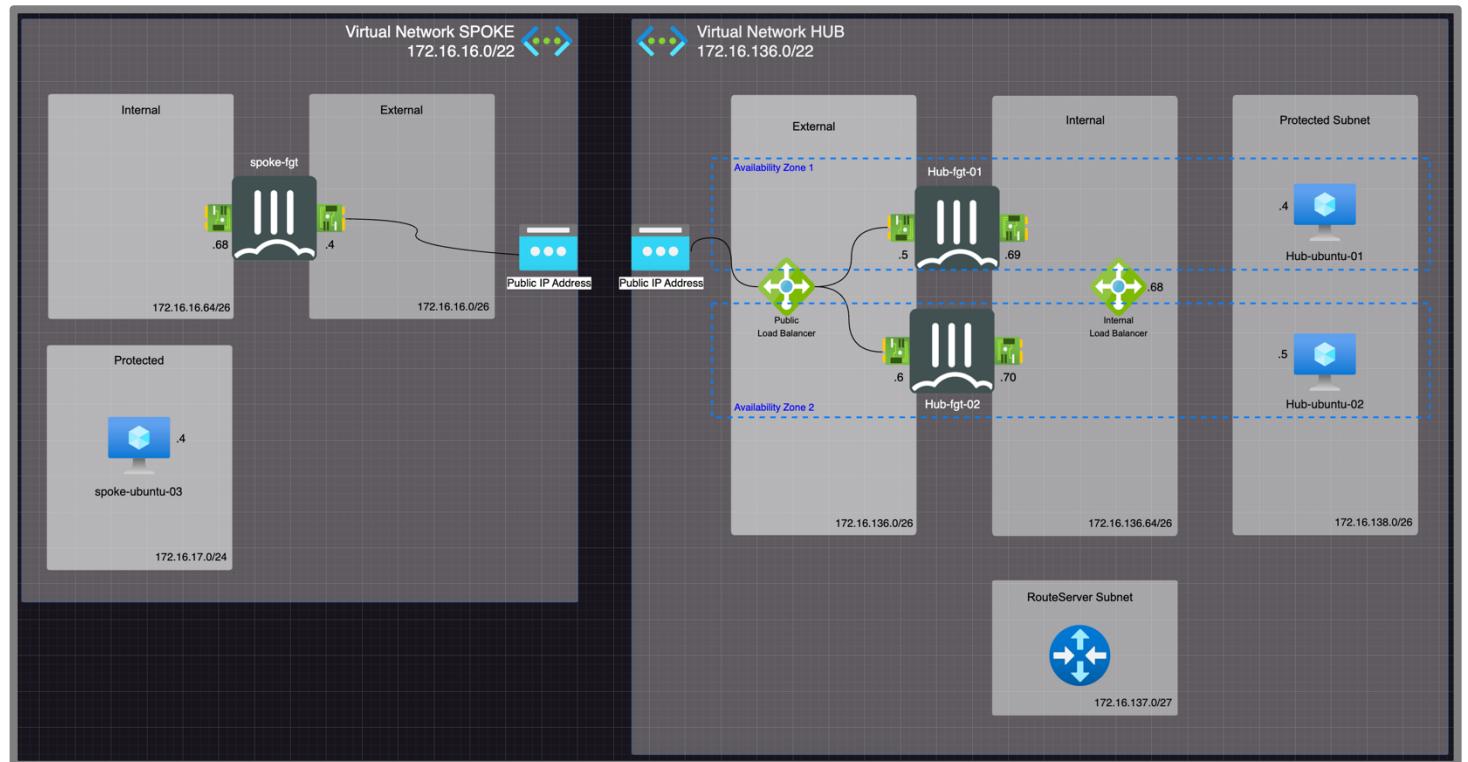


1 Fortigate @AZURE lab

1.	<i>Creazione account console Azure</i>	3
1.1.	Accesso Portale Azure	4
2.	<i>Resource Group</i>	9
3.	<i>HUB - Creazione cluster Fortigate Active/Active</i>	10
4.	<i>HUB - Creazione Azure Route Server</i>	13
5.	<i>HUB - Creazione server Ubuntu01</i>	16
6.	<i>HUB - Accesso server Ubuntu01 tramite VIP cluster</i>	18
6.1.	TEST	21
7.	<i>SPOKE - Creazione Fortigate single-vm</i>	22
8.	<i>SPOKE - Creazione server Ubuntu03</i>	25
9.	<i>SPOKE - Accesso server Ubuntu03 tramite VIP Fortigate spoke</i>	27
10.	<i>Configurazione BGP all'interno della vnet HUB</i>	29
10.1.	TEST	30
11.	<i>Configurazione VPN tra HUB e SPOKE</i>	32
11.1.	creazione regole di load balancing	32
11.2.	configurazione ipsec sui fortigate hub	33
11.3.	configurazione interfaccia ipsec sui fortigate hub	33
11.4.	configurazione bgp sui fortigate hub	34
11.5.	configurazione secondary ip address sui fortigate hub	34
11.6.	creazione regola sui fortigate hub	34
11.7.	configurazione ipsec su fortigate spoke	34
11.8.	configurazione interfaccia ipsec su fortigate spoke	35
11.9.	configurazione bgp su fortigate spoke	35
11.10.	creazione regola su fortigate spoke	35
11.11.	TEST	35
11.12.	TEST	36
12.	<i>HUB - Microsegmentazione</i>	38
12.1.	Installazione di un nuovo server hub-ubuntu-02	38
12.2.	Creazione e configurazione nuova routing table	41
12.3.	TEST	43
12.4.	Creazione policy per traffico EST-OVEST	44
12.5.	TEST	44
13.	<i>Segmentazione con VNET Peering</i>	45
13.1.	Creazione nuova VNET son una subnet Protected	45
13.2.	Creazione nuove VM all'interno delle nuove VNET	47
13.3.	Creazione nuova Route Table da associare alle nuove Subnet	50
13.4.	Configurazione VNET Peering	52
13.5.	Impostare il routing sui due Fortigate HUB	53
13.6.	Creazione Policy sui due Fortigate HUB	53
13.7.	TEST	54
14.	<i>Rimozione risorse</i>	55



1. Creazione account console Azure

Un partecipante per ogni coppia acceda al link o scansioni il qrcode con il proprio smartphone:

<https://forms.office.com/e/6ppruZQxE1>



Inserire la mail di uno dei due partecipanti: su questa mail verranno inviate le credenziali di accesso all'account Azure e le licenze Fortigate (verificare ricezione mail anche nella cartella spam)

The screenshot shows a Microsoft Forms survey titled "Fortinet Xperts Summit 2024". It contains one question: "1. Email *". A text input field is provided for the answer, with the placeholder "Enter your answer". Below the input field is a "Submit" button. At the bottom of the form, there is a Microsoft 365 logo and a privacy statement: "This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password." It also mentions "Microsoft Forms | AI-Powered surveys, quizzes and polls" and "The owner of this form has not provided a privacy statement as to how they will use your response data. Do not provide personal or sensitive information." There is a link to "Report abuse".

Una volta compilato il form verrà inviata una mail contenente:

Nome Utente: userXXX@itxperts.it

Password: *****

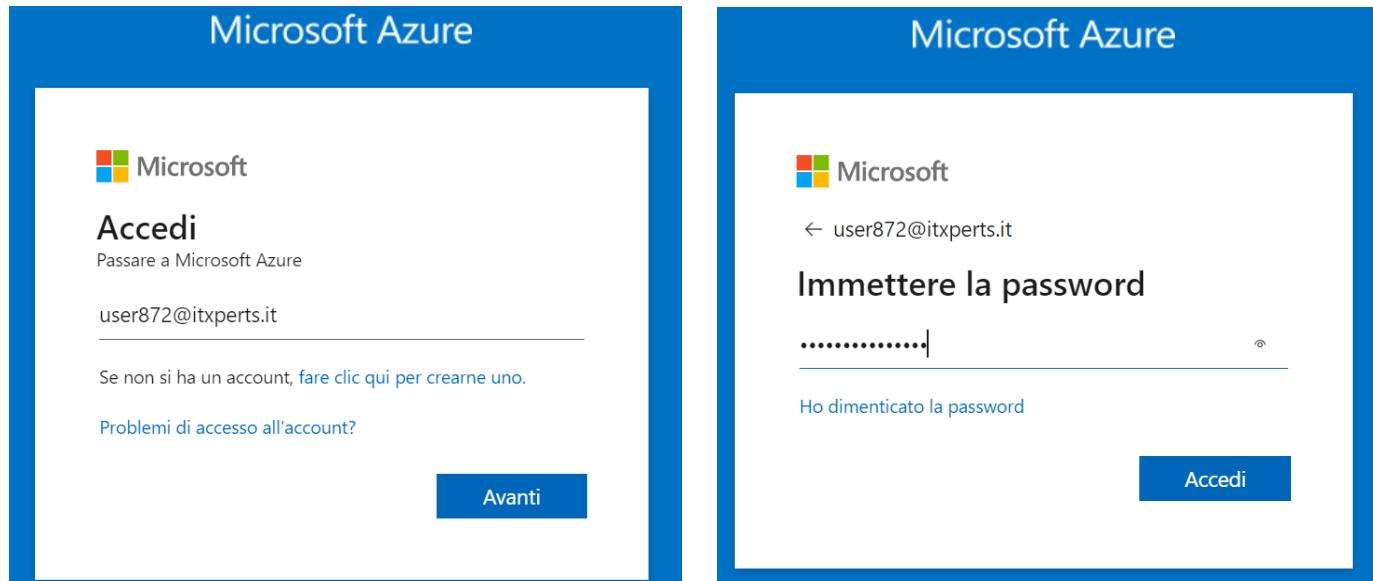
N.B. Alla medesima casella verranno inviati, in un secondo momento, le licenze da utilizzare sui Fortigate durante il laboratorio

1.1. Accesso Portale Azure

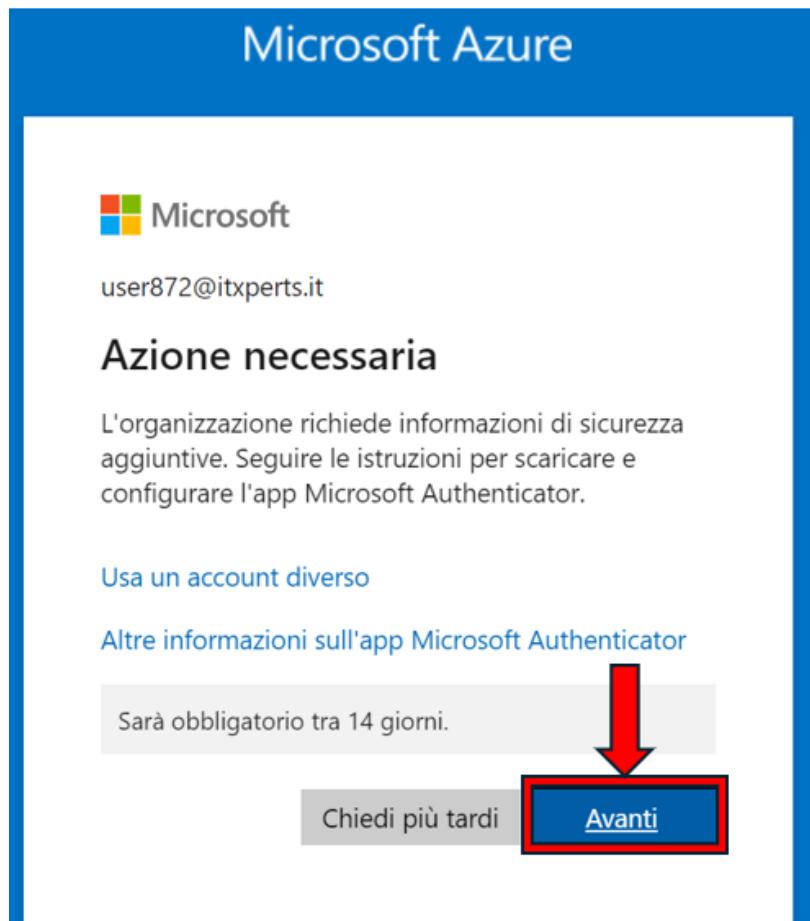
Una volta ottenute le credenziali via email collegarsi alla pagina di login di Azure:

<https://portal.azure.com>

Inserire l'utenza e la password ricevute via mail



Alla richiesta di Azione Necessaria selezionare AVANTI



Se non già presente installare sullo smartphone di uno dei due partecipanti l'app **Microsoft Authenticator**.

Microsoft Authenticator



Ottenerne prima di tutto l'app

Nel telefono installare l'app Microsoft Authenticator. [Scarica ora](#)

Dopo l'installazione dell'app Microsoft Authenticator nel dispositivo, scegliere "Avanti".

[Voglio usare un'app di autenticazione diversa](#)

[Avanti](#)

Scarica l'app sul tuo smartphone*

Scansiona il codice a matrice con il tuo dispositivo mobile Android o iOS.



Aprire l'app sullo smartphone e cliccare su “+” in alto a destra. Dopodiché selezionare “**Account aziendale o dell'istituto di istruzione**” e cliccare su “**Scansione codice QR**”

The figure consists of three screenshots of the Microsoft Authenticator app. The first screenshot shows the main screen with a list of accounts and a blue '+' button at the top right. The second screenshot shows the 'Aggiungi account' (Add account) screen with three options: 'Account personale', 'Account aziendale o dell'istituto di istruzione' (which is highlighted with a red box), and 'Altro (Google, Facebook e così via)'. The third screenshot is a modal dialog titled 'Aggiungi account aziendale o dell'istituto di istruzione' with three buttons: 'Accedi', 'Scansione codice QR' (which is highlighted with a red box), and 'Annulla'.

Da portale web selezionare **Avanti**, di nuovo **Avanti** e scannerizzare il **QR Code** mostrato a portale dallo smartphone e cliccare nuovamente su **Avanti** (esempio sotto)

Microsoft Authenticator



Ottenere prima di tutto l'app

Nel telefono installare l'app Microsoft Authenticator. [Scarica ora](#)

Dopo l'installazione dell'app Microsoft Authenticator nel dispositivo, scegliere "Avanti".

[Voglio usare un'app di autenticazione diversa](#)

Avanti →

Microsoft Authenticator



Configura l'account

Se richiesto, consentire le notifiche. Aggiungere quindi un account e selezionare "Account aziendale o dell'istituto di istruzione".

Indietro → Avanti

Microsoft Authenticator

Esegui la scansione del codice a matrice

Usare l'app Microsoft Authenticator per eseguire la scansione del codice a matrice. L'app Microsoft Authenticator verrà connessa all'account.

Dopo la scansione del codice a matrice, scegliere "Avanti".

ESEMPIO



Non è possibile digitalizzare l'immagine?

Indietro → Avanti

Viene richiesto di verificare un numero sull'app Microsoft Authenticator.

Sullo Smartphone aprire l'app Microsoft Authenticator e inserite il codice mostrato sulla pagina web.

Microsoft Authenticator

Prova

Per approvare la notifica inviata all'app, immettere il numero visualizzato di seguito.

22

Indietro Avanti



Stai provando ad accedere?

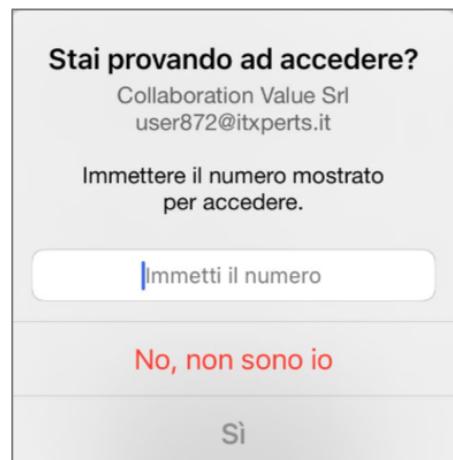
Collaboration Value Srl
user872@itxperts.it

Immettere il numero mostrato per accedere.

Immetti il numero

No, non sono io

Sì

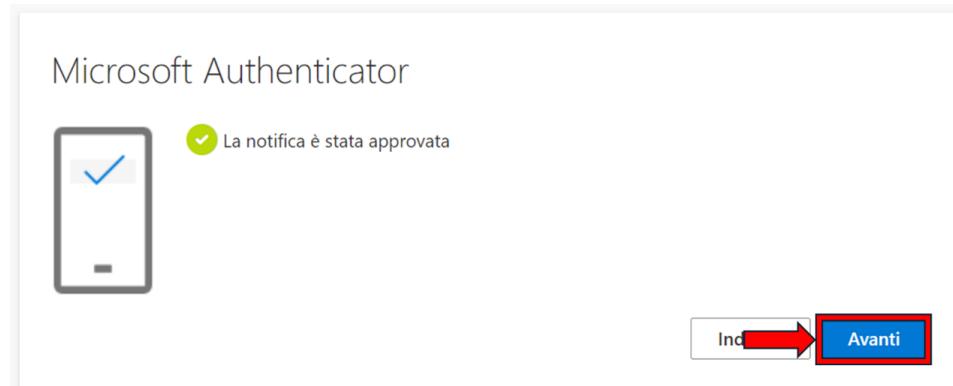


Selezionare **Avanti** e **Fine**

Microsoft Authenticator

La notifica è stata approvata

Ind Avanti



Operazione riuscita

Le informazioni di sicurezza sono state configurate. Scegliere "Fine" per continuare la procedura di accesso.

Metodo di accesso predefinito:

 Microsoft Authenticator

Ind Fine



Saltare le domande di intro del portale Azure (skip)

Accesso alla console di Azure

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar, and various navigation icons. Below the header, a row of service icons includes 'Crea una risorsa', 'Centro di avvio rapido', 'Macchine virtuali', 'Servizi app', 'Account di archiviazione', 'Database SQL', 'Azure Cosmos DB', 'Servizi Kubernetes', 'App per le funzioni', and 'Altri servizi'. The main content area is titled 'Risorse' and has tabs for 'Recenti' (selected) and 'Preferiti'. It displays a message: 'Non sono state visualizzate risorse di recente' with a button 'Visualizza tutte le risorse'.

Attenzione!

Il laboratorio contiene riferimenti a servizi in lingua inglese. Per poter seguire in maniera corretta tutte le parti del laboratorio è consigliato seguire le seguenti istruzioni al fine di impostare la lingua in inglese.

Per poter cambiare lingua all'interfaccia andare (da portale Azure come in figura sopra) in alto a destra sull' icona di impostazioni si aprirà una finestra come in figura sotto; da lì selezionare sulla sinistra “**Lingua e area Geografica**”. Scegliere sotto lingua “**English**” e sotto formato regionale “**English (United States)**” e successivamente cliccare su **Applica**. Come ultima cosa ci verrà chiesto di confermare l'impostazione della lingua; clicchiamo su **OK** e il portale verrà ricaricato con le corrette impostazioni

The screenshot shows the 'Impostazioni del portale | Directory e sottoscrizioni' (Portal settings | Directories and subscriptions) page. On the left, there's a sidebar with links like 'Menu Cerca', 'Directory e sottoscrizioni' (which is selected and highlighted with a red box), 'Aspetto e visualizzazioni di avvio', 'Lingua e area geografica' (also highlighted with a red box), 'Informazioni personali', 'Collegamenti utili', and 'Invia commenti'. The main content area has sections for 'Filtro sottoscrizioni predefinito' (Subscription filter), 'Filtri avanzati' (Advanced filters), and 'Directory' (which is currently set to 'Collaboration Value Srl'). There are also tables for 'Preferiti' (Favorites) and 'Tutte le directory' (All directories). The 'Tutte le directory' table includes columns for 'Nome directory' (Name), 'Corrente' (Current), 'Dominio' (Domain), and 'ID directory' (ID).

Microsoft Azure Cerca risorse, servizi e documentazione (G+) Copilot

Impostazioni del portale | Lingua e area geografica

Menu Cerca Scegliere la lingua e il formato regionale per determinare la modalità di visualizzazione di data/ora e valuta.

Directory e sottoscrizioni Lingua English ↘

Aspecto e visualizzazioni di avvio Formato regionale English (United States) ↘

Lingua e area geografica

Informazioni personali

Collegamenti utili

- Altre informazioni sulle impostazioni ↗
- Includi gli URL nell'elenco di indirizzi attendibili ↗
- Microsoft Partner Network
- Informativa sulla privacy ↗
- Dichiarazione di accessibilità ↗
- Altre risorse di Azure
- Invia commenti

Applica Rimuovi modifiche

English

English (United States)

Applica

Rimuovi modifiche

Modifica lingua

Applicare queste modifiche alle impostazioni della lingua e dell'area? Il portale verrà ricaricato e verranno applicate queste impostazioni.

OK

Annulla

Tornare alla pagina iniziale cliccando su **Microsoft Azure** in alto a sinistra.

2. Resource Group

Con la creazione dell'utente viene creato anche un proprio Resource Group con nome **RG-<utente>** all'interno del quale verranno installate tutte le risorse del lab.

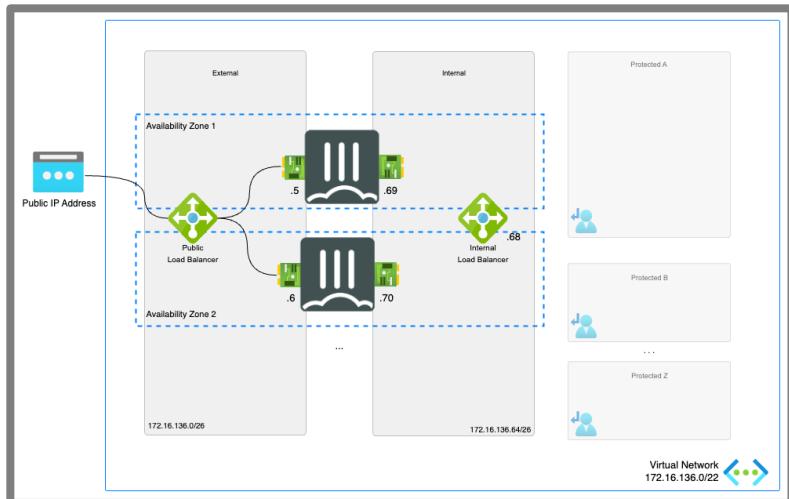
3. HUB - Creazione cluster Fortigate Active/Active

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

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**.

Azure Portal

Selezionare **Deploy to Azure**

Custom deployment: [Deploy to Azure](#)

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

Subscription * ⓘ

Resource group * ⓘ

SE-Subscription

abcd22

Create new

Instance details

Region * ⓘ

(Europe) Italy North

Admin Username * ⓘ

abcd22

Admin Password * ⓘ

Forti Gate Count ⓘ

2

Forti Gate Name Prefix * ⓘ

hub

Forti Gate Image Sku ⓘ

fortinet_fg-vm

Forti Gate Image Version ⓘ

latest

Forti Gate Additional Custom Data ⓘ

Forti Gate Session Sync ⓘ

false

Forti Gate Probe Response ⓘ

true

Instance Type ⓘ

Standard_F2s

External Load Balancer ⓘ

true

Outbound Connectivity ⓘ

external-nat-device-or-elb

Availability Options ⓘ

Availability Zones

Accelerated Networking ⓘ

true

Accelerated Connections ⓘ

false

Accelerated Connections Sku ⓘ

A1

Compilare il form come in figura:

Selezionare il proprio Resource Group.

Inserire la username amministrativa (si consiglia uguale all'username dell'account azure)

Inserire la password (se si perde non sarà possibile recuperarla).

La password deve essere almeno 6 caratteri e rispettare le seguenti regole, altrimenti il deploy fallisce.

- 1) Contains an uppercase character
- 2) Contains a lowercase character
- 3) Contains a numeric digit
- 4) Contains a special character

Per esempio : Fortinet!<username azure>

Inserire **hub** come prefisso .

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

Vnet Name ⓘ

hub-abcd22

Vnet Resource Group ⓘ

Vnet Address Prefix ⓘ

172.16.136.0/22

Subnet1Name ⓘ

externalsubnet

Subnet1Prefix ⓘ

172.16.136.0/26

Subnet1Start Address ⓘ

172.16.136.4

Subnet2Name ⓘ

internalsubnet

Subnet2Prefix ⓘ

172.16.136.64/26

Subnet2Start Address ⓘ

172.16.136.68

Subnet3Name ⓘ

protectedsubnet

Subnet3Prefix ⓘ

172.16.138.0/26

Serial Console ⓘ

yes

Forti Manager ⓘ

no

Vnet Name : hub-<username azure>
(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 type="text"/> 9BC3828CC6C26F7D989B ✓
Forti Gate License Forti Flex2 ⓘ	<input 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"/> {} ✓
Fortinet Tags	<input type="text"/> {"publisher":"Fortinet","template":"Active-Active-ELB-ILB","provider":"6... ✓
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input style="background-color: #0072BD; color: white; font-weight: bold; border-radius: 5px; padding: 2px 10px; border: none;" type="button" value="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**

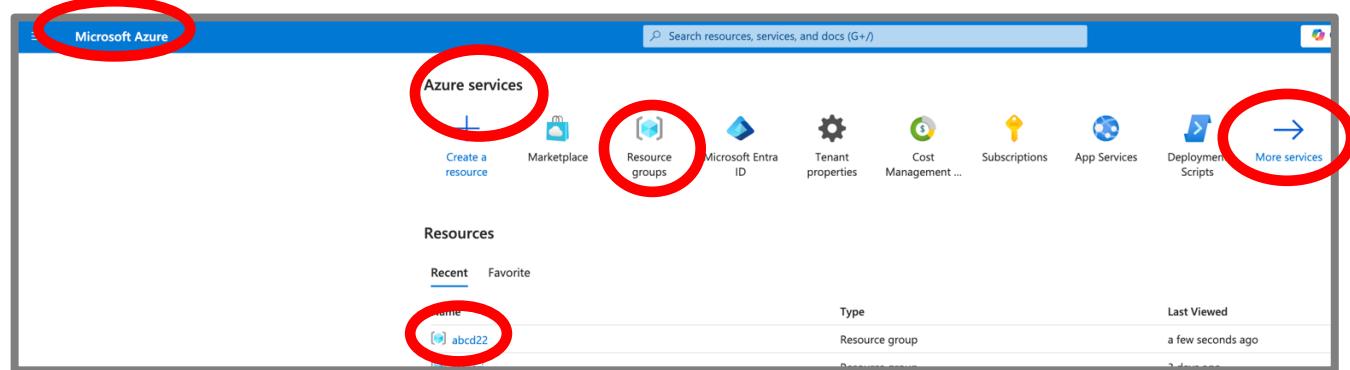
Selezionare **Create**

4. 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 a destra su **Microsoft Azure** (sempre presente in qualunque schermata della console) e successivamente selezionare il proprio resource Group (da elenco Recent o da Azure Service -> More Services)



Name	Type	Last Viewed
abcd22	Resource group	a few seconds ago

Type
Virtual network
Virtual machine
Virtual machine
Route table
Public IP address
Public IP address
Public IP address
Network security group
Network Interface
Network Interface
Network Interface
Network Interface
Load balancer
Load balancer
Disk

Cliccare sul nome della colonna Type per mettere in ordine le risorse.

Selezionare la Virtual Network hub-xxxxxx

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

Note: 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 <small>[PREVIEW]</small>	
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)	<input type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/> Give feedback	

Inserire 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 **Create a Resource** o **Marketplace** (Azure Service -> more Service, oppure digitare Marketplace nel search in alto al centro nella barra blu)

Microsoft Azure

Home >

Marketplace

Get Started

Service Providers

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Security (15)

azur

Azure services only

Showing 1 to 20 of 21 results for 'azur'

Route Server

Microsoft

Azure Service

Azure Route Server simplifies dynamic routing between your network virtual appliance (NVA) and your virtual network.

Create

Route Server

Nel campo search del Marketplace o del New Resource digitare **Azure route server** e dare invio.

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

Create a Route Server

Subscription *: SE-Subscription

Resource group *: abcd22 (Create new)

Instance details

Name *: ARSabcd22

Region *: Italy North

Routing Preference *: ExpressRoute VPN ASPath

Note: Route Server will prefer the connection with the shortest AS Path.

Configure virtual networks

Virtual network *: hub-abcd22 (Create new)

Subnet *: RouteServerSubnet (172.16.137.0/27) (Manage subnet configuration)

Public IP address

Public IP address *: Create new Use existing

Public IP address name *: hub-abcd22-ip

Buttons: Review + create, Previous, Next : Tags >, Download a template for automation

Compilare i parametri come da figura a fianco.

Usare come nome del router

ARS<username azure>

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 utilizzata per i test.

5. HUB - Creazione server Ubuntu01

Tornare nella Home della console Azure e entrare nel Marketplace.

Nel campo search digitare **ubuntu server 22.04** 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 LTS (Canonical)**-> **Create**

(attenzione **NON** selezionare Ubuntu Minimal)

Instance details

Virtual machine name * ✓

Region * ✓

Availability options ✓

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](#)
 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

Size *

Compilare i parametri scorrendo le opzioni fino in fondo.

Resource Group : confermare vostro Resource Group

VM name: hub-ubuntu-01

Security Type: Standard

Size: B1ms

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.

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

Authentication Type: Password

Impostare username = username
azure

Impostare password:

es -> Fortinet!<username azure>

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

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](#)

Networking

Compilare i parametri di rete come da figura

Selezionare

La propria HUB-vnet

ProtectedSubnet

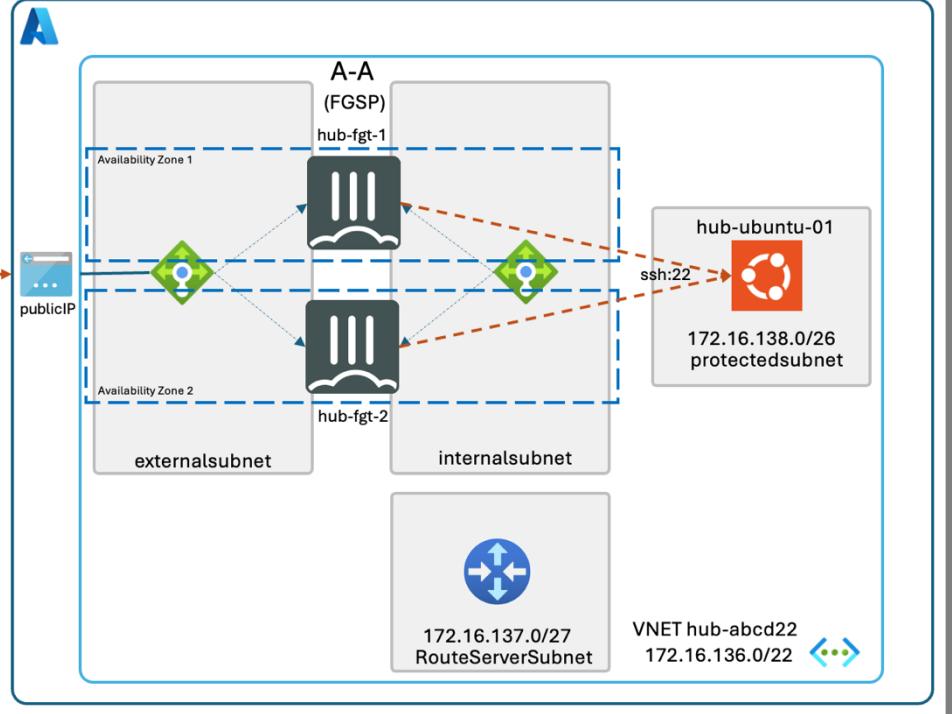
NIC security Group: None

No Public IP

Review + create

Create

6. 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. In the 'Resources' section, a resource group named 'abcd22' is highlighted with a red circle. Other resources listed include 'loadbalancer', 'hub-fgt-2', 'hub-fgt-1', 'hub-ubuntu-01', 'FG-FGT', 'ubu', 'FG-FGT-Nic1', 'external', 'nat', 'natgw', and 'fcaliari'. The 'abcd22' resource group is listed as a Resource group, last viewed a few seconds ago.

Name	Type	Last Viewed
abcd22	Resource group	a few seconds ago
loadbalancer	Load balancer	15 minutes ago
hub-fgt-2	Virtual machine	15 hours ago
hub-fgt-1	Virtual machine	15 hours ago
hub-ubuntu-01	Virtual machine	15 hours ago
FG-FGT	Virtual machine	15 hours ago
ubu	Virtual machine	15 hours ago
FG-FGT-Nic1	Network interface	15 hours ago
external	Route table	15 hours ago
nat	NAT gateway	15 hours ago
natgw	Public IP address	15 hours ago
fcaliari	Resource group	15 hours ago

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

The screenshot shows the Azure portal interface for a resource group named 'abcd22'. In the left sidebar, under 'Load balancer', the 'hub-externalloadbalancer' resource is selected. The main content area displays the 'Load balancing rules' section. A table lists three existing rules: 'ExternalLBRule-FE-http' (Protocol: TCP/80), 'ExternalLBRule-FE-udp10551' (Protocol: UDP/10551), and another unnamed rule (Protocol: UDP). A search bar and a filter by name bar are also present.

The screenshot shows the 'Add load balancing rule' dialog. The configuration parameters are as follows:

- 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
- Outbound source network address translation (SNAT):
 - (Recommended) Use outbound rules to provide backend pool members access to the internet. [Learn more](#).
 - (Selected) 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. [Learn more](#).

At the bottom are 'Save' and 'Cancel' buttons.

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

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 inserito al lancio del template.

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

```
config firewall vip
edit vip_20022
    set extip x.x.x.x (indirizzo ip pubblico del External Load Balancer)
    set mappedip 172.16.138.4
    set extintf port1
    set portforward enable
    set extport 20022
    set mappedport 22
next
end
config firewall service custom
edit tcp_20022
    set tcp-portrange 20022
next
end
```

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

```
config firewall address
edit myip
    set associated-interface port1
    set subnet x.x.x.x 255.255.255.255
next
end

config firewall policy
edit 1
    set name ssh_ubntu
    set srcintf port1
    set dstintf port2
    set action accept
    set srcaddr myip
    set dstaddr vip_20022
```

```

        set schedule always
        set service SSH tcp_20022
        set nat enable
    next
end

```

La regola deve avere il source nat per due motivi:

- 1- 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 .
- 2- 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.

6.1. 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.

Uscire dalla sessione ssh e 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.

7. 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

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)

Blockchain (0)

Search: fortigate byol

Pricing: All

Operating System: All

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

Offer	Provider	Description	Pricing	Action
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
Azure Virtual WAN Secured by Fortinet FortiGate	Fortinet	Azure Application FortiGate NVA 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

Single VM

Active-Passive HA with Fabric Connector Failover

Active-Active Loadbalanced with ELB Single VM

Active-Passive HA with ELB/ILB

Nel campo search digitare **Fortigate BYOL**

In Fortinet Fortigate Next-Generation Firewall, selezionare

Create -> Single VM

Basics Instance Networking Public IP Advanced 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

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

Compilare i parametri come da figura a fianco.

Resource Group

Italy North

Usare sempre le stesse username e password

Spoke

Next

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

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

Virtual Machine Name

Name of the FortiGate VM

Previous **Next** **Review + create**

Selezionare **Fortiflex** e inserire terzo token ricevuto via mail.

Next

Basics **Instance** **Networking** **Public IP** **Advanced** **Review + create**

Configure Internal Networking

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

Virtual network **Edit virtual network**

External Subnet * **Edit subnet** 172.16.16.0 - 172.16.16.63 (64 addresses)

Internal subnet * **Edit subnet** 172.16.16.64 - 172.16.16.127 (64 addresses)

Protected subnet * **Edit subnet** 172.16.17.0 - 172.16.17.255 (256 addresses)

Il template crea automaticamente una VNET con 3 subnet.

Edit virtual network per modificare la vnet

Home > abcd22 > Marketplace > Create Single VM >

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](#)

Add IPv4 address space

172.16.16.0/22	<input type="button" value="Delete address space"/>		
This address prefix overlaps with virtual network 'AZG-VNET'. If you intend to peer these virtual networks, change the address space. Learn more			
172.16.16.0	/22		
172.16.16.0 - 172.16.19.255	1,024 addresses		
<input type="button" value="Add a subnet"/>			
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	/28 (64 addresses)	-
ProtectedSubnet	172.16.17.0 - 172.16.17.255	/24 (256 addresses)	-

Nel campo nome inserire **spoke-<username>**

Modificare indirizzamento vnet con

172.16.16.0/22

Automaticamente vengono aggiornate le subnet

SAVE

NEXT

Basics **Instance** **Networking** **Public IP** **Advanced** **Review + create**

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 **Create new**

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.

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

Create public IP address

Name * ✓

SKU * (1)
 Basic Standard

Routing preference (1)
 Microsoft network Internet

Impostare i parametri come in figura

in basso a destra selezionare **OK**

Review + create -> Create

The screenshot shows the Azure Notifications page. At the top, there is a header with icons for Home, Notifications (circled in red), Settings, Help, and Search. Below the header, the title is "Notifications". There is a link to "More events in the activity log". A deployment message is displayed: "Deployment succeeded Deployment 'fortinet.fortinet-fortigate-20240724080' group 'abcd22' was successful." At the bottom, there are two buttons: "Pin to dashboard" and "Go to resource group".

Attendere qualche minuto per permettere al deployment di terminare la creazione di tutte 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.

Nella sezione overview è possibile recuperare l'IP pubblico.

The screenshot shows the Azure Virtual Machine overview page for the "spoke-FGT" VM. The left sidebar has links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Network settings, and Load balancing. The main area has tabs for Overview, Activity log, and Essentials. In the Essentials tab, there is a table with the following data:

Operating system	: Linux (FortiOS v7.4.4)
Public IP address	4.232.144.110
Virtual network/subnet	: spoke-VNET/ExternalSubnet
DNS name	: spoke-fgt-ztpaotmt6z2.italynorth.cloudapp.azure.com
Health state	: -
Time created	: 7/19/2024, 9:39 AM UTC

At the bottom, there is a note: "Tags (edit) provider : 6EB3B02F-50E5-4A3E-8CB8-2E12925831VM".

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).

8. 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 ...

Get Started

Service Providers

Azure services only

Management

Showing 1 to 20 of 1604 results for 'ubuntu server'

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Compute (540)

Developer Tools (461)

Create

Ubuntu Server 22.04 LTS

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

Subscription * ⓘ SE-Subscription

Resource group * ⓘ abcd22

Create new

Instance details

Virtual machine name * ⓘ spoke-ubuntu-03

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](#).

Compilare i parametri scorrendo le opzioni fino in fondo.

Run with Azure Spot discount

Size * Standard_B1ms - 1 vcpu, 2 GiB memory (\$17.52/month)

Enable Hibernation
Info 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

Info 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

Usare sempre le stesse credenziali

Username Azure

Password: Fortinet!<username>

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 * spoke-abcd22

Subnet * ProtectedSubnet (172.16.17.0/24)

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

< Previous

Networking

Compilare i parametri di rete come da figura.

Selezionare

La vnet **spoke-<name>**

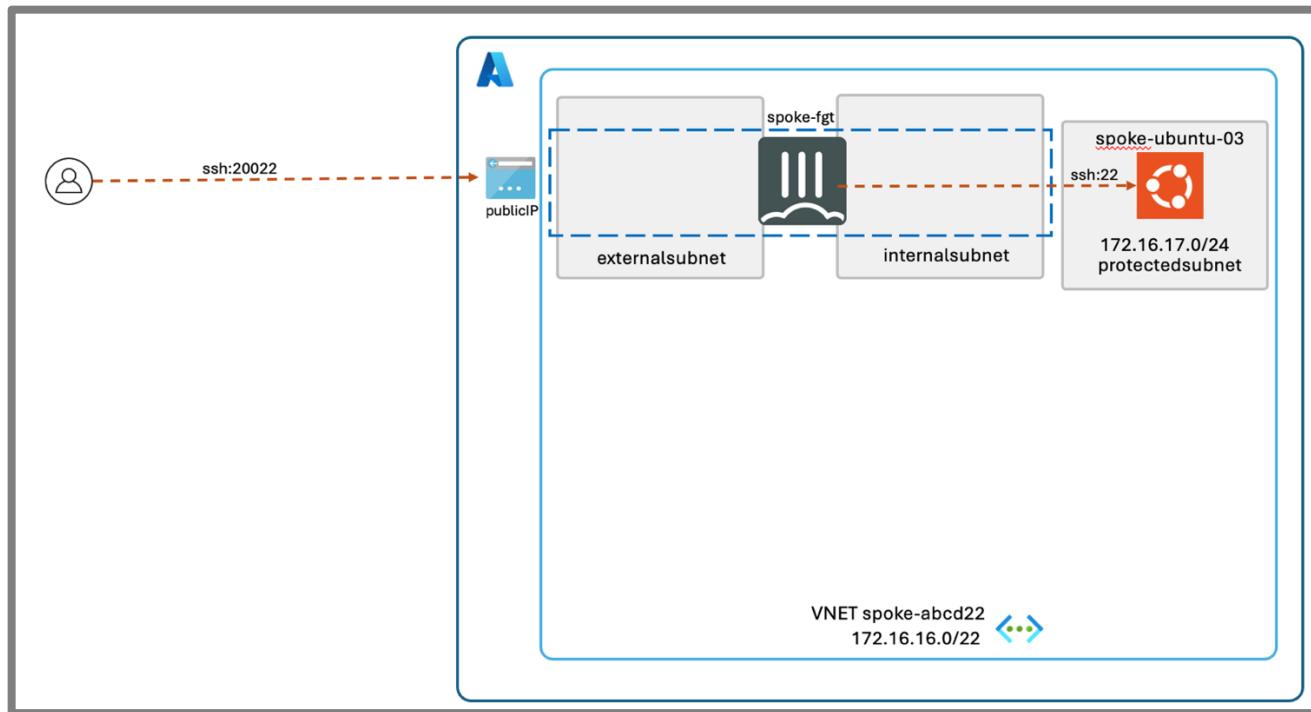
ProtectedSubnet

No Public IP

Review + create

Create

9. 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 (Il tutto è stato creato automaticamente mediante template)

[Home > abcd22 > spoke-VNET](#)

spoke-VNET | Subnets ☆ ...

Virtual network

Name	IPv4	IPv6	Available IPs	Delegated to	Sec...	Route table
ExternalSubnet	172.16.16.0/26	-	58	-	-	-
InternalSubnet	172.16.16.64/26	-	58	-	-	-
ProtectedSubnet	172.16.17.0/24	-	250	-	-	spoke-RouteTable-ProtectedSubnet

[Home > abcd22 > spoke-VNET | Subnets >](#)

spoke-RouteTable-ProtectedSubnet ☆ ...

Route table

Overview																			
Associations : 1 subnet associations																			
Essentials																			
Resource group : abcd22	Location : Italy North	Subscription (move) : SE-Subscription	Tags (edit) : provider:6EB3B02F-50E5-4A3E-8CB8-2E12925831VM																
Routes																			
<table border="1"> <thead> <tr> <th>Name</th> <th>Address prefix</th> <th>Next hop type</th> <th>Next hop IP address</th> </tr> </thead> <tbody> <tr> <td>Default</td> <td>0.0.0.0/0</td> <td>Virtual appliance</td> <td>172.16.16.68</td> </tr> <tr> <td>Subnet</td> <td>172.16.17.0/24</td> <td>Virtual network</td> <td>-</td> </tr> <tr> <td>VirtualNetwork</td> <td>172.16.16.0/22</td> <td>Virtual appliance</td> <td>172.16.16.68</td> </tr> </tbody> </table>				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
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																
Subnets																			
<table border="1"> <thead> <tr> <th>Name</th> <th>Address range</th> <th>Virtual network</th> <th>Security group</th> </tr> </thead> <tbody> <tr> <td>ProtectedSubnet</td> <td>172.16.17.0/24</td> <td>spoke-VNET</td> <td>-</td> </tr> </tbody> </table>				Name	Address range	Virtual network	Security group	ProtectedSubnet	172.16.17.0/24	spoke-VNET	-								
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.

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).

```
config firewall vip_20022
    edit vip_spoke
        set mappedip 172.16.17.4
        set extintf port1
        set portforward enable
        set extport 20022
        set mappedport 22
    next
end
```

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

```
config firewall service custom
    edit tcp_20022
        set tcp-portrange 20022
    next
end

config firewall address
    edit myip
        set associated-interface port1
        set subnet x.x.x.x 255.255.255.255
    next
end

config firewall policy
    edit 1
        set name ssh_ubuntu
        set srcintf port1
        set dstintf port2
        set action accept
        set srcaddr myip
        set dstaddr vip_20022
        set schedule always
        set service SSH tcp_20022
        set nat enable
    next
end
```

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

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

10. 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 Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main area is titled 'Resources' and shows a list of resources. One resource, 'ARSabcd22', is highlighted with a red box. Other resources listed include 'hub-abcd22-ip', 'hub-externalloadbalancer-pip', 'spoke-FGT-PIP', 'hub-routetable', 'spoke-RouteTable-ProtectedSubnet', and 'hub-fgt-1'. There are also buttons for 'Create', 'Manage view', and 'Delete resource' at the top.

Dalla lista delle risorse all'interno del proprio Resource Group selezionare **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 (with Configuration and Peers sub-options), and Properties. The main area has sections for 'Essentials' (Resource group: abcd22, Location: italynorth, Subscription: SE-Subscription, Provisioning State: Succeeded, Connectivity Status: Succeeded, Virtual Network / Subnet: ARSabcd22) and 'Peers' (ASN: 65515, Peer Ips: 172.16.137.5, 172.16.137.4). A red box highlights the 'Peers' section.

(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 settings. The left sidebar shows 'Peers' selected. The main area has a search bar, an 'Add' button (highlighted with a red box), and a refresh button. Below is a table with columns for 'Name' and 'No results'. The sidebar also includes Configuration and Properties options.

Nel menu a sinistra del Route Server selezionare

Settings -> Peers

Nel menu in alto selezionare **ADD**

Add Peer

Name * hub-fgt-1

ASN * 65400

IPv4 Address * 172.16.136.69

Add Peer

Name * hub-fgt-2

ASN * 65400

IPv4 Address * 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>

10.1. 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 dal template (le rotte statiche hanno distanza preferenziale)

Controllare le rotte statiche sui fortigate hub

Destination	Gateway IP	Interface	Status
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

Su entrambi i FGT HUB 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

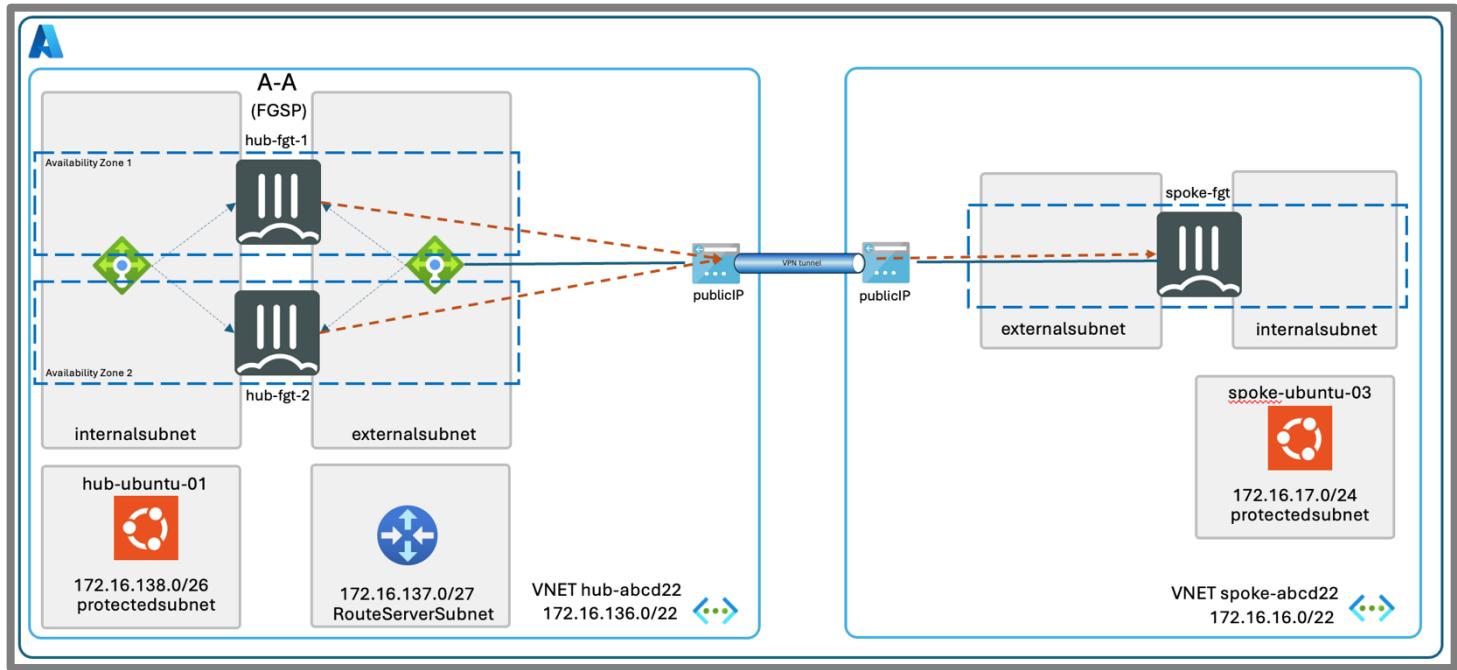
Edit Static Route

Destination	<input checked="" type="radio"/> Subnet <input type="radio"/> Internet Service
	172.16.137.0/255.255.255.224
Gateway Address	172.16.136.65
Interface	port2 <input type="button" value="x"/>
Administrative Distance	10
Comments	Write a comment... 0/255
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<input type="checkbox"/> Advanced Options	

Da CLI verificare la ricorsività della network 172.16.136.0/22

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

11. 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.

11.1. 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

11.2. 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
```

11.3. 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
```

11.4. 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.

11.5. 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/32 (Ip pubblico dell'Externalloadbalancer)
            next
        end
    next
end
```

11.6. 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
```

11.7. 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.

11.8. 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
```

11.9. 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
```

11.10. 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
```

11.11. TEST

Accedere al server spoke-Ubuntu-03

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

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)



2.

(selezionare powershell)

All'interno della shell digitare sequenzialmente i due comandi:

```
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

3. 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 Attach network interface Detach network interface View topology

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

Connect Networking

Network settings (selected) Load balancing Application security groups Network manager

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.

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

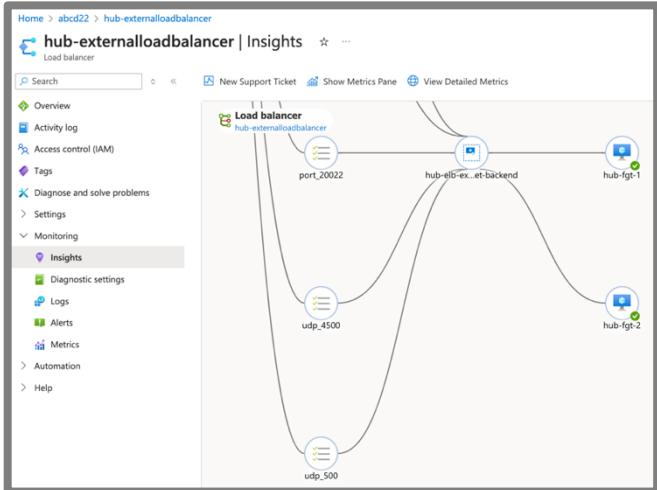
11.12. TEST

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

Spegnere il nodo che sta gestendo la VPN:

il bilanciatore si accorge del fail in 10..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**

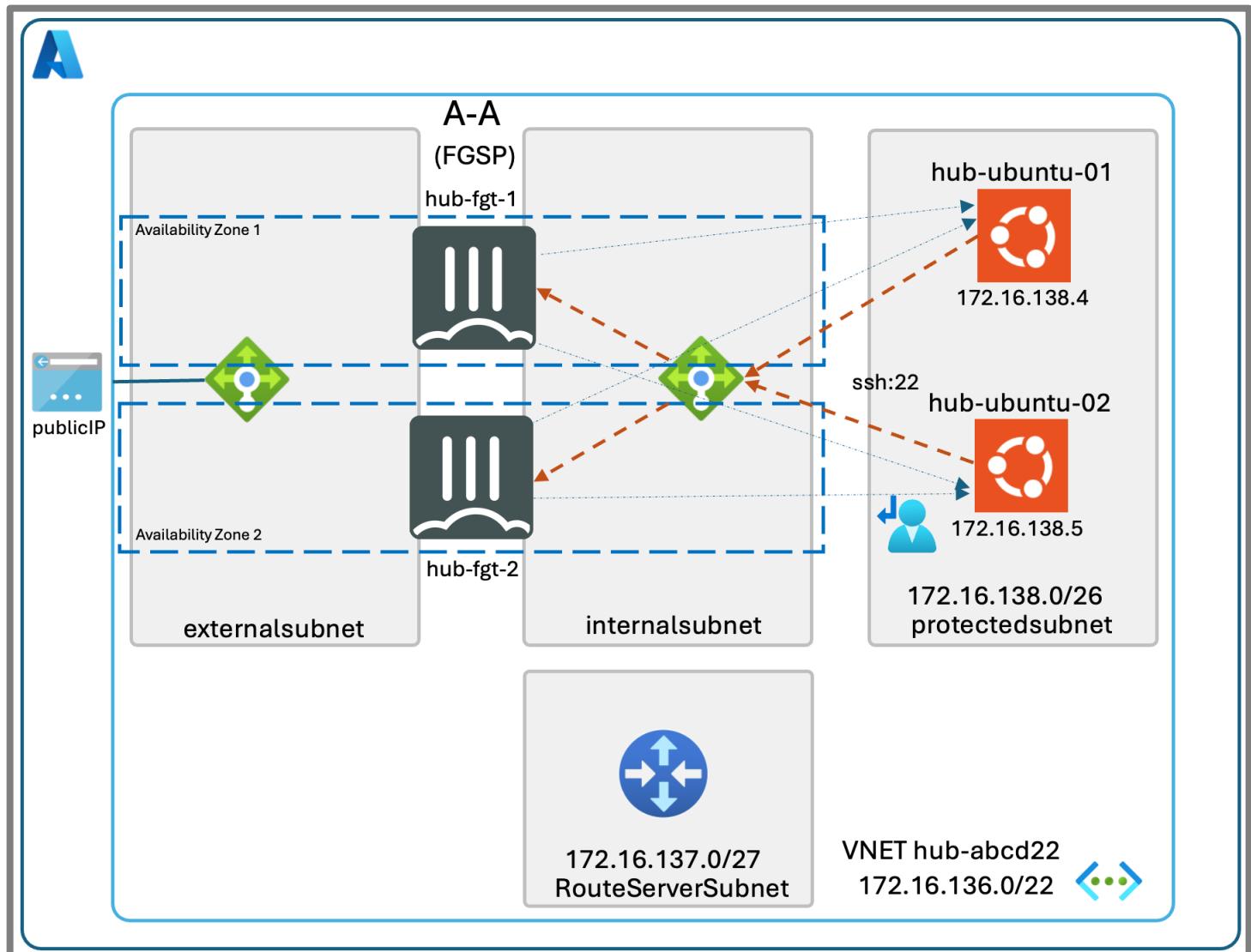
Fare zoom sulle icone dei due nodi fortigate.

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.

12. HUB - Microsegmentazione



Scopo dell'esercizio è applicare la network security tra due server installati nella stessa subnet.

Una delle caratteristiche di Azure è la possibilità di sfruttare lo User Defined Routing in modo che possa avere la priorità sulla subnet stessa in cui viene applicata. Questo permette di ottenere la microsegmentazione, ovvero la possibilità di controllare sul Fortigate le comunicazioni tra server installati nella stessa subnet.

Task dell'esercizio:

- installazione del server hub-ubuntu-02 nella Protected Subnet (la stessa di hub-ubuntu-01)
- configurazione nuova routing table (UDR) da associare alla Protected Subnet
- configurazione policy sui due nodi hub-fgt per permettere l'SSH
- test flussi (SSH ->ok , PING ->ko)

12.1. 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

The screenshot shows the Azure Marketplace search interface. A search bar at the top contains the text "ubuntu server". Below the search bar, there is a checkbox labeled "Azure services only". The main area displays search results for "ubuntu server", showing two items: "Ubuntu Server 22.04 LTS" and "Ubuntu Server 20.04 LTS", both offered by Canonical as Virtual Machines for Linux For The Cloud.

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

The screenshot shows the "Basics" tab of the Azure VM creation wizard. It includes fields for "Subscription" (set to "SE-Subscription"), "Resource group" (set to "abcd22"), "Virtual machine name" (set to "hub-ubuntu-02"), "Region" (set to "(Europe) Italy North"), "Availability options" (set to "Availability zone"), "Availability zone" (set to "Zone 2"), "Security type" (set to "Standard"), and "Image" (set to "Ubuntu Server 22.04 LTS - x64 Gen2"). A note indicates that multiple zones can be selected to create one VM per zone.

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 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

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.

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

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

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](#)

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 (sempre tramite vip_20022) e da qui verificare che sia tramite ping sia tramite ssh si raggiunge hub-ubuntu-02

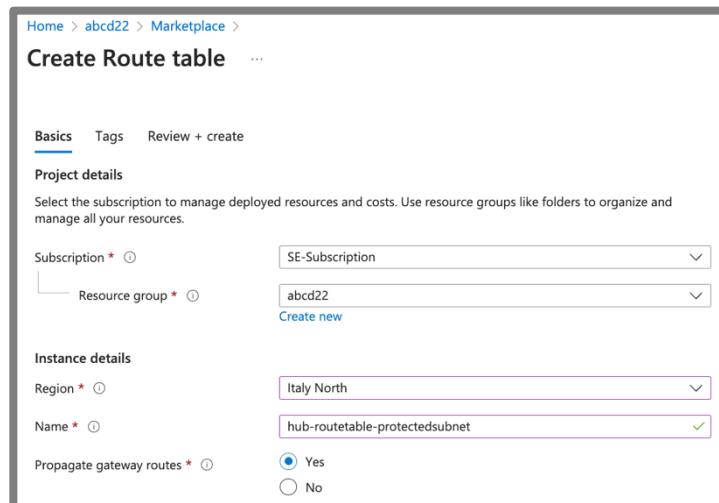
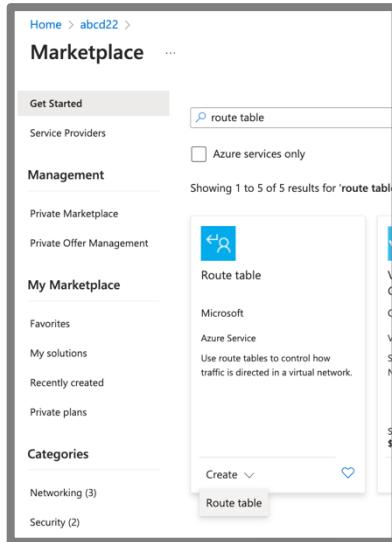
```
ssh abcd22@x.x.x.x -p 20022
```

```
ping 172.16.138.5
```

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

12.2. Creazione e configurazione nuova routing table

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

Resource Group

Italy North

Nome

Review + create

Create

I prossimi step prevedono l'inserimento nella routing table del default GW verso l'ip del load balancer interno e l'associazione della routing table alla Protected Subnet.

Per recuperare l'ip del load balancer interno tornare alla Home e all'elenco delle risorse, selezionare

hub-internalloadbalancer

Home > abcd22 >

hub-internalloadbalancer

Load balancer

Search ▾ Move Delete Refresh Give feedback

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Monitoring
- Automation
- Help

Resource group (move) : abcd22

Location : Italy North

Subscription (move) : SE-Subscription

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

SKU : Standard

Tags (edit)

See more

Selezionare **See more**

L'ip appare a destra

Home > abcd22 >

hub-internalloadbalancer

Load balancer

Search ▾ Move Delete Refresh Give feedback

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Monitoring
- Automation

Tags (edit)

: publisher : Fortinet | template : Active-Active-ELB-ILB | provider : 6EB3B02F-50E5-4A3E-8CB8-2E12925831AA

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

Tornare al setup della routing table selezionando **hub-routetable-protectedsubnet** dall'elenco delle risorse

Home > abcd22 > hub-routetable-protectedsubnet

hub-routetable-protectedsubnet

Route table

Search ▾ Associate

Subnets

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Properties

Locks

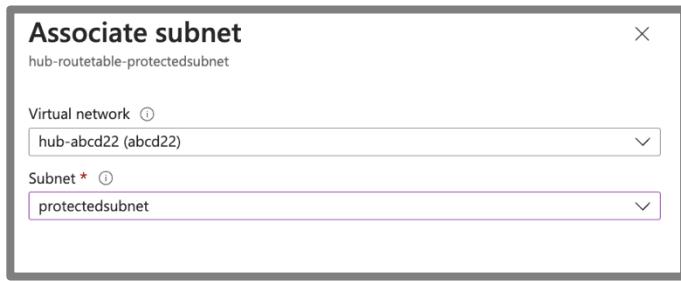
Monitoring

Automation

Help

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

Dal menu in alto selezionare **Associate**



Selezionare la propria Vnet hub e la protectedsubnet.

OK

Il prossimo step prevede l'inserimento della rotta statica per ruotare la protectedsubnet via indirizzo del loadbalancer interno.

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

Dal menu in alto selezionare **Add**

Inserire i parametri come in figura.

Il destination IP address Range è esattamente l'indirizzo della protected subnet cui viene applicata la rotta statica.

Add

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

12.3. TEST

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

```

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

```

12.4. Creazione policy per traffico EST-OVEST

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

```

config firewall address
edit hub-ubuntu-01
    set associated-interface port2
    set subnet 172.16.138.4 255.255.255.255
next
edit hub-ubuntu-02
    set associated-interface port2
    set subnet 172.16.138.5 255.255.255.255
next
end

config firewall policy
edit 3
    set name microsegmentation
    set srcintf port2
    set dstintf port2
    set action accept
    set srcaddr hub-ubuntu-01
    set dstaddr hub-ubuntu-02
    set schedule always
    set service SSH
next
end

```

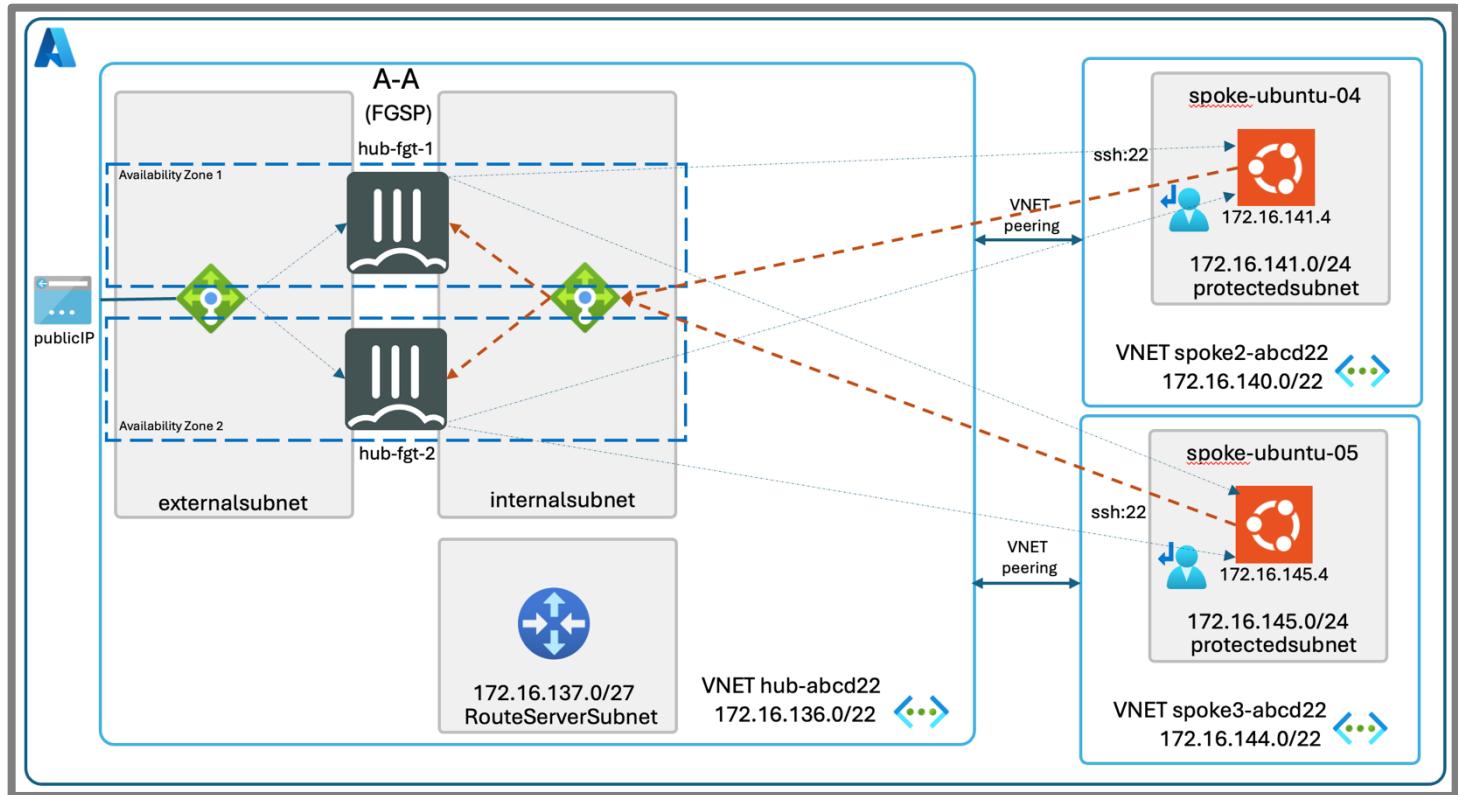
Non è necessario abilitare il NAT poiché le sessioni est-ovest attraversano solo il bilanciatore interno.

12.5. 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.

13. Segmentazione con VNET Peering



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

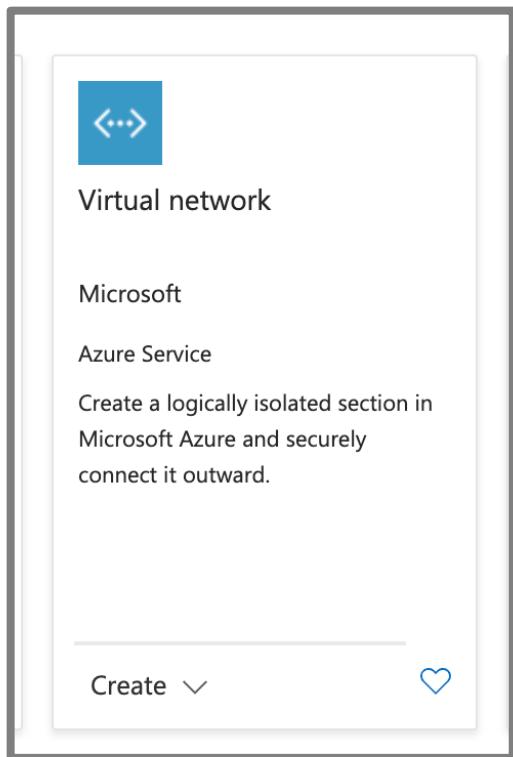
Task dell'esercizio:

- 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

13.1. 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-<username>

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
	Create new

Instance details

Virtual network name *	spoke2-abdc22
Region * ⓘ	(Europe) Italy North
Deploy to an Azure Extended Zone	

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

The screenshot shows the Azure portal interface for creating a virtual network. On the left, there's a navigation bar with 'Home > fmfm11 > Marketplace > Create virtual network'. Below it, tabs for 'Basics', 'Security', 'IP addresses' (which is selected), 'Tags', and 'Review + create' are visible. The main area is titled 'Add a subnet'.

Subnet purpose: Default

Name: protectedsubnet

IPv4:

- Include an IPv4 address space:** checked
- IPv4 address range:** 172.16.140.0/22 (selected)
- 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:** unchecked (checkbox)
- Note:** This virtual network has no IPv6 address ranges.

Private subnet: PREVIEW

Note: 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): checkbox (unchecked)

Review + Create -> Create

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

13.2. Creazione nuove VM all'interno delle nuove VNET

Installare un nuovo server spoke2-ubuntu-04.

Tornare nella Home della console AZURE e entrare nel Marketplace.

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

The screenshot shows the Azure Marketplace interface. A search bar at the top contains the text "ubuntu server". Below the search bar, there is a checkbox labeled "Azure services only". On the left, a sidebar includes sections for "Get Started", "Service Providers", "Management", "Private Marketplace", "Private Offer Management", "My Marketplace" (which is currently selected), "Favorites", "My solutions", "Recently created", "Private plans", and "Categories" (with options for Compute and Developer Tools). The main area displays search results for "ubuntu server", showing two items: "Ubuntu Server 22.04 LTS" by Canonical and "Ubuntu Server 20.04 LTS" by Canonical. Both items are listed as "Virtual Machine" types under "Linux For The Cloud". Each item has a "Create" button below it.

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

This screenshot shows the first step of the Azure VM creation wizard. It includes fields for "Virtual machine name" (spoke-ubuntu-04), "Region" ((Europe) Italy North), "Availability options" (Self-selected zone selected), "Zone options" (Zone 1 selected), "Availability zone" (Zone 1), "Security type" (Trusted launch virtual machines), and "Image" (Ubuntu Server 22.04 LTS - x64 Gen2).

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 vnet spoke2

ProtectedSubnet

No Public IP

Review + create

Create

Ripetere le stesse operazioni per una nuova VM da nominare come spoke3-ubuntu-05 e posizionarla nella subnet protected subnet della VNET Spoke3

13.3. 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 main results area displays one item: 'Route table' by Microsoft, categorized under 'Azure Service'. The description states: 'Use route tables to control how traffic is directed in a virtual network.' At the bottom of the card, there is a 'Create' button with a dropdown arrow and a blue heart icon.

Create Route Table

Dare il nome RTspokeVNET-<username>

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 *	<input type="text" value="Default"/> ✓
Destination type *	<input type="text" value="IP Addresses"/> ✓
Destination IP addresses/CIDR ranges *	<input type="text" value="0.0.0.0/0"/> ✓
Next hop type *	<input type="text" value="Virtual appliance"/> ✓
Next hop address *	<input type="text" value="172.16.136.68"/> ✓

i 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 le due subnet “protected subnet” della VNET spoke2-abcd22 e della VNET spoke3-abcd22.

Associate subnet

X

RTspokeVNET-fmfm11

Virtual network ⓘ

spoke2-fmfm11 (fmfm11) ✓

Subnet * ⓘ

protectedsubnet ✓

OK

Ripetere per la protected subnet della vnet spoke3.

13.4. 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

Add peering ...

hub-user118

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. This will allow resources in either virtual network to directly connect and communicate with resources in the peered virtual network.

Remote virtual network summary

Peering link name *	peering-hub-to-spoke2
Virtual network deployment model ⓘ	<input checked="" type="radio"/> Resource manager <input type="radio"/> Classic
I know my resource ID ⓘ	<input type="checkbox"/>
Subscription *	Azure subscription 1
Virtual network *	spoke2-118 (RG-User118)

Remote virtual network peering settings

- Allow 'spoke2-118' to access 'hub-user118'
- Allow 'spoke2-118' to receive forwarded traffic from 'hub-user118'
- Allow gateway or route server in 'spoke2-118' to forward traffic to 'hub-user118'
- Enable 'spoke2-118' to use 'hub-user118's remote gateway or route server

Local virtual network summary

Peering link name *

Local virtual network peering settings

Allow 'hub-user118' to access 'spoke2-118' ⓘ

Allow 'hub-user118' to receive forwarded traffic from 'spoke2-118' ⓘ

Allow gateway or route server in 'hub-user118' to forward traffic to 'spoke2-118' ⓘ

Enable 'hub-user118' to use 'spoke2-118's' remote gateway or route server ⓘ

[Add](#) [Cancel](#)

Fare Add

Ripetere per la VNET Spoke3.

13.5. Impostare il routing sui due Fortigate HUB

Il next Hop per 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.

```
config router static
  edit 5
    set dst 172.16.141.0 255.255.255.0
    set gateway 172.16.138.65
    set device port2
  next
  edit 6
    set dst 172.16.145.0 255.255.255.0
    set gateway 172.16.138.65
    set device port2
  next
end
```

13.6. Creazione Policy sui due Fortigate HUB

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.

```
config firewall address
edit spoke-ubuntu-04
  set associated-interface port2
  set subnet 172.16.141.4 255.255.255.255
next
edit spoke-ubuntu-05
  set associated-interface port2
  set subnet 172.16.145.4 255.255.255.255
next
end
```

```
config firewall policy
edit 20
    set name segmentazione-vnet
    set srcintf port2
    set dstintf port2
    set action accept
    set srcaddr spoke-ubuntu-04 spoke-ubuntu-05
    set dstaddr spoke-ubuntu-04 spoke-ubuntu-05
    set schedule always
    set service SSH
next
end
```

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

13.7. TEST

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

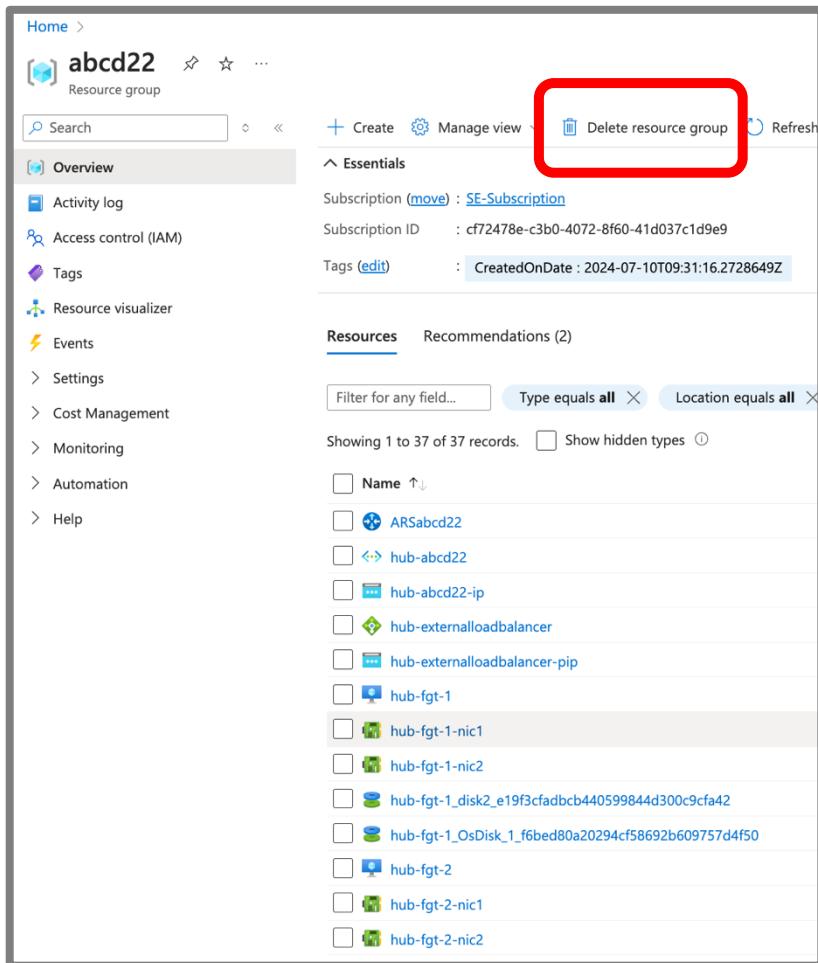
Da spoke-ubuntu-04 fare ping verso spoke-ubuntu-05 (172.16.145.4), il ping non risponde poiché viene bloccato dal firewall

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

14. Rimozione risorse

Prima di concludere il LAB rimuovere tutte le risorse create.

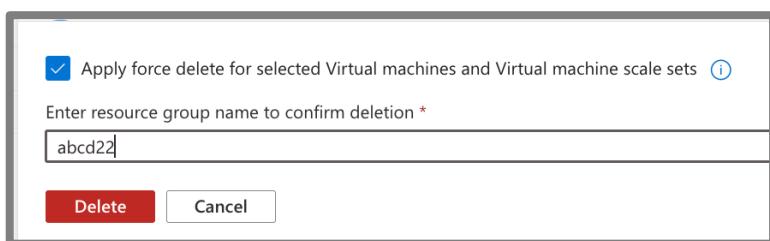
Dalla home selezionare il proprio resource group



The screenshot shows the Azure Resource Group Overview page for a group named 'abcd22'. The left sidebar contains navigation links like Home, Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main area displays subscription details (Subscription (move) : SE-Subscription, Subscription ID : cf72478e-c3b0-4072-8f60-41d037c1d9e9, Tags (edit) : CreatedOnDate : 2024-07-10T09:31:16.2728649Z) and a list of resources under the 'Resources' tab. The 'Delete resource group' button in the top right corner is highlighted with a red box.

nel menu in alto selezionare

Delete resource group



The screenshot shows a confirmation dialog box. At the top, there is a checked checkbox labeled 'Apply force delete for selected Virtual machines and Virtual machine scale sets' with an information icon. Below it is a text input field with the placeholder 'Enter resource group name to confirm deletion *' and the value 'abcd22' entered. At the bottom of the dialog are two buttons: a red 'Delete' button and a white 'Cancel' button.

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