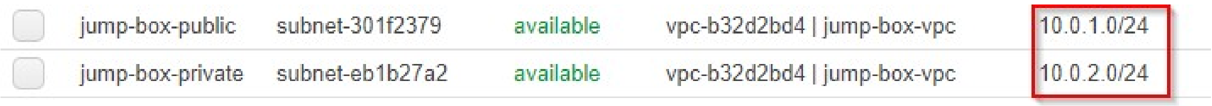
How to protect a private subnet by using a jump-box instance

Objective is to isolate a private subnet by allowing it to be accessed only via a dedicated jump-box server.

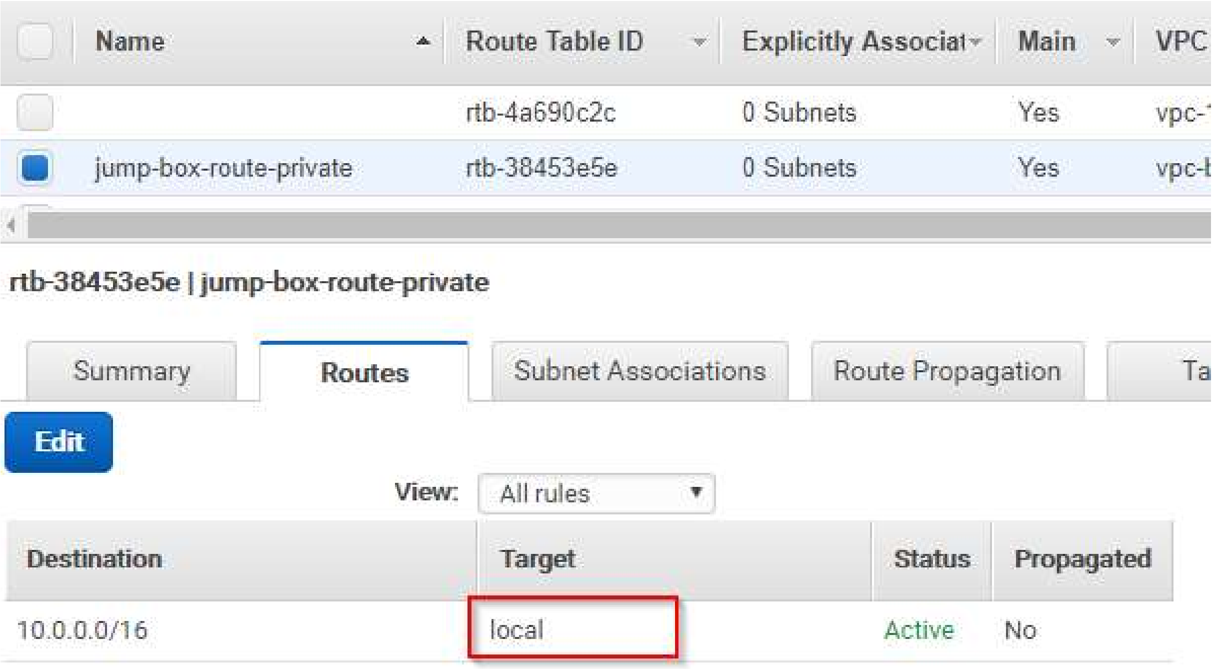
Following landscape has to be set-up:

2 subnets, a public and a private one, with corresponding route tables



□	jump-box-public	subnet-301f2379	available	vpc-b32d2bd4 | jump-box-vpc	10.0.1.0/24
□	jump-box-private	subnet-eb1b27a2	available	vpc-b32d2bd4 | jump-box-vpc	10.0.2.0/24

Private route table has only local target



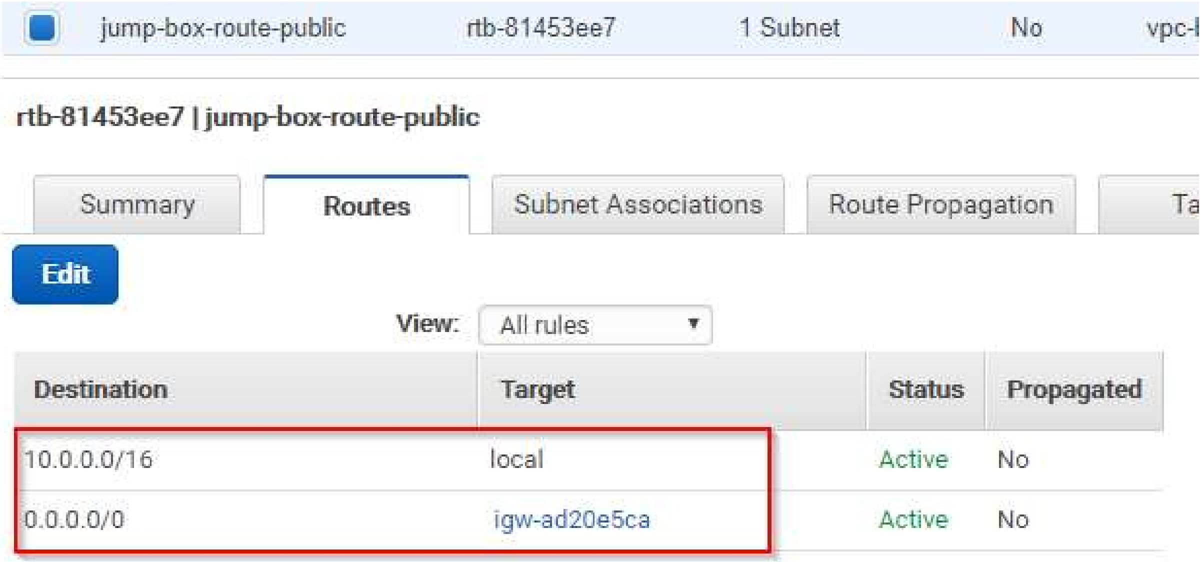
□	Name	Route Table ID	Explicitly Associat	Main	VPC
□		rtb-4a690c2c	0 Subnets	Yes	vpc-'
☑	jump-box-route-private	rtb-38453e5e	0 Subnets	Yes	vpc-l

rtb-38453e5e | jump-box-route-private

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

A public route table with the internet gateway as target



☑	jump-box-route-public	rtb-81453ee7	1 Subnet	No	vpc-l

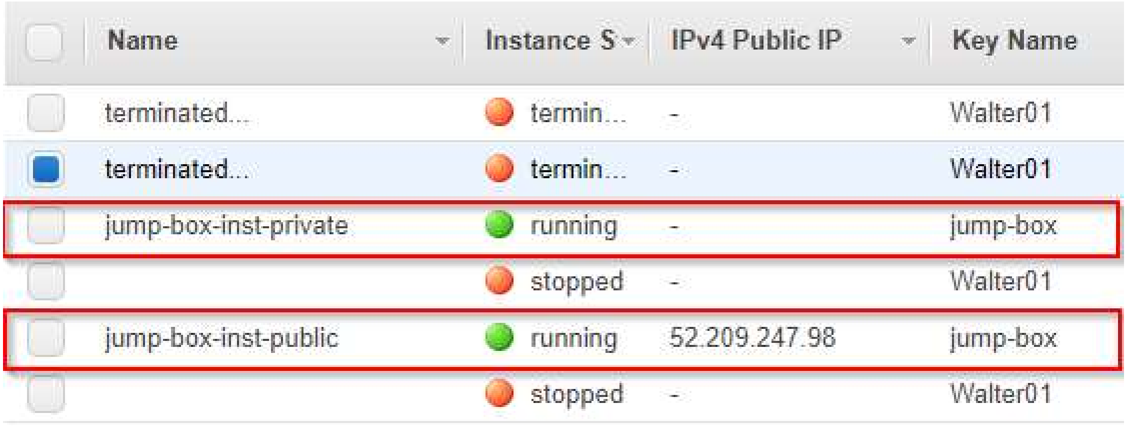
rtb-81453ee7 | jump-box-route-public

View: All rules ▼

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-ad20e5ca	Active	No

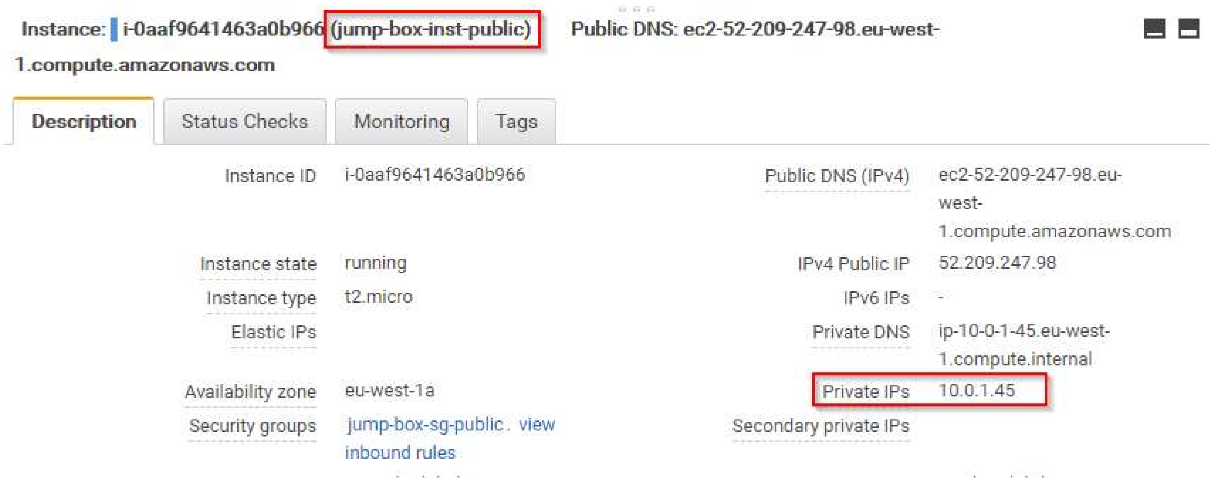
Two server instances are created.

Public one, with security group allowing SSH from anywhere, and a private one, allowing SSH only from the private IP of the public instance.



□	Name	Instance S	IPv4 Public IP	Key Name
□	terminated...	● termin...	-	Walter01
☑	terminated...	● termin...	-	Walter01
□	jump-box-inst-private	● running	-	jump-box
□		● stopped	-	Walter01
□	jump-box-inst-public	● running	52.209.247.98	jump-box
□		● stopped	-	Walter01

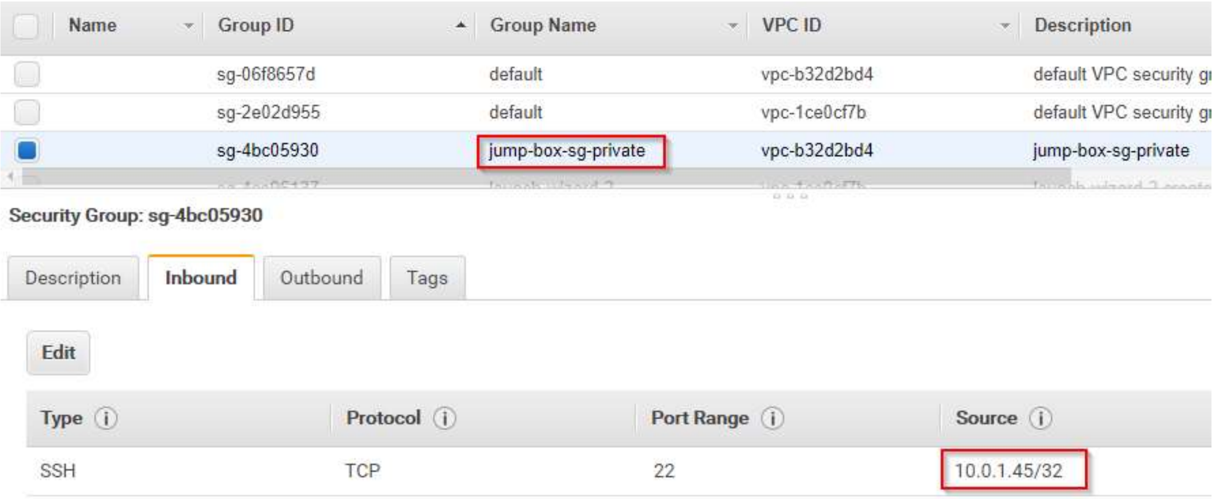
Details of public instance



Instance: i-0aaf9641463a0b966 (jump-box-inst-public) Public DNS: ec2-52-209-247-98.eu-west-1.compute.amazonaws.com

Instance ID	i-0aaf9641463a0b966	Public DNS (IPv4)	ec2-52-209-247-98.eu-west-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	52.209.247.98
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-10-0-1-45.eu-west-1.compute.internal
Availability zone	eu-west-1a	Private IPs	10.0.1.45
Security groups	jump-box-sg-public. view inbound rules	Secondary private IPs	

Security group of private instance



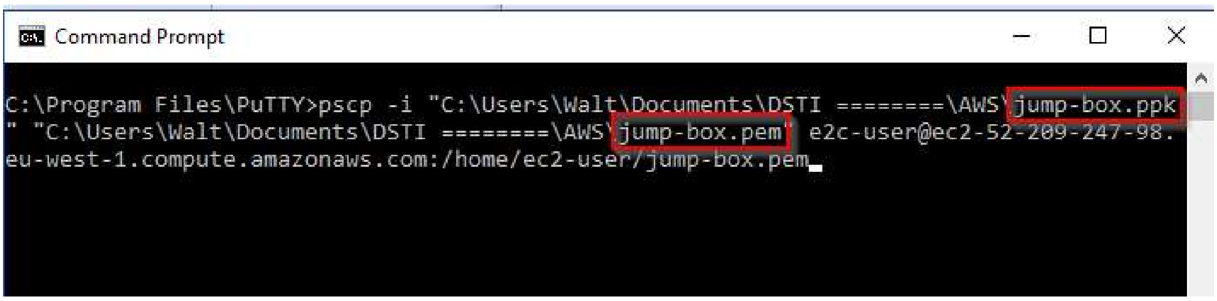
Name	Group ID	Group Name	VPC ID	Description
	sg-06f8657d	default	vpc-b32d2bd4	default VPC security gr
	sg-2e02d955	default	vpc-1ce0cf7b	default VPC security gr
	sg-4bc05930	jump-box-sg-private	vpc-b32d2bd4	jump-box-sg-private

Security Group: sg-4bc05930

Type	Protocol	Port Range	Source
SSH	TCP	22	10.0.1.45/32

Using Puttygen, convert PEM file into PPK file.

Then use Putty utility PSCP to copy the PEM file of the private instance to a folder of the public instance.



```
C:\Program Files\PuTTY>pscp -i "C:\Users\Walt\Documents\DSTI ========\AWS\jump-box.ppk
" "C:\Users\Walt\Documents\DSTI ========\AWS\jump-box.pem" e2c-user@ec2-52-209-247-98.
eu-west-1.compute.amazonaws.com:/home/ec2-user/jump-box.pem
```

We are then able to connect via ssh from public instance to private instance, using its pem file.

References

What's a Jump Box?

https://userify.com/docs/advanced/jumpbox/

Securely Connect to Linux Instances Running in a Private Amazon VPC

https://aws.amazon.com/blogs/security/securely-connect-to-linux-instances-running-in-a-private-amazon-vpc/

USING PSCP TO TRANSFER FILES SECURELY

https://www.ssh.com/ssh/putty/putty-manuals/0.68/Chapter5.html