Laboratory Practice Report

Practice 3

September 20, 2023

Computer Systems Engineering

Cloud Architecture

Prof. M.S. Rodolfo Luthe Ríos

Marco Ricardo Cordero Hernández

is727272@iteso.mx

ITESO

Universidad Jesuita
de Guadalajara

Abstract

The current work has the objective of providing a demonstration of virtual private networks usage and utility within cloud technologies in order to address multiple concerns such as security, privacy, consistency, administration, exploration of remote infrastructure, etc.

Although a deep level of detail isn't provided and background knowledge won't be needed for its understanding, the material found as useful for this development and its actual elaboration intends to provide the reader with enough material to replicate its contents.

An historical overview will also be provided to understand what it's being accomplished together with individual objectives that attend to several potential use cases for future projects that involves granular access. This, along with the revisited concept of bastion instance, intends to demonstrate the possible reach of the particular tools explored here.

Finally, reflections about the development and its involvements will be held to demonstrate understanding of the accomplishments succeeded, as this particular topic regarding cloud technologies could be significantly useful or harmful, this being by how it could be handled.

State of the Art

In the beginning of what now it's known as the internet as a whole, in the decade of the 60's, there was an intent from the government to share research information between remote collaborators [1]. Back then, portable computers would still be a faraway concept, as mainframes dominated the scene [2], leaving scientists and researchers with two uncomfortable options: traveling directly to the resource of interest, or, have send it over mail in the form of magnetic tapes.

What ultimately made the first step into an appropriate solution was the creation of the "*Advanced Research Projects Agency Network*", better know as ARPANET, the technology that would evolve into today's main mean of communication. But, before evolving into a public resource, this network was only available for academic and research organizations, something that lead into the creation of more networks intended for multiple purposes.

Even then, as it can be seen, the roots of internet were something secluded, and only available for user segments, and although this was an evident limitation and thus an improvement area, in the context of its creation it was seen as a feature, as something desirable [3], because *privacy* was desirable at the internet's creation. When standard protocols, such as the "*Transmission Control Protocol* and Internet Protocol" [TCP/IP] were formally introduced back in 1983 to ARPANET [4], a whole new range of possibilities started to arise, as well as new technologies such as routers and concepts as gateways. In any kind of development, specially as huge as the one that it's being discussed, as it becomes larger and incorporates new technologies, new vulnerabilities come along with them; among the most popular of them, when referring to network vulnerabilities, are malware, outdated software, and misconfigured firewalls [5]. Surely, in an educative or demonstrative environment such as the one found within this development, this wouldn't suppose a high level threat, however, in production, enterprise assets such as data and code bases shouldn't be *public*.

Now, a new question arises, even when internet access it's almost considered as a human right [6], would all of its contents need to be accessible to the public domain? Certainly not, as what now has become the massive data cluster that is the internet, contains top secret documents that would even suppose the fall of contemporary regimes. But, does the solution to these high risk operations need to be an overkill, expensive and complex? Yet again, certainly not.

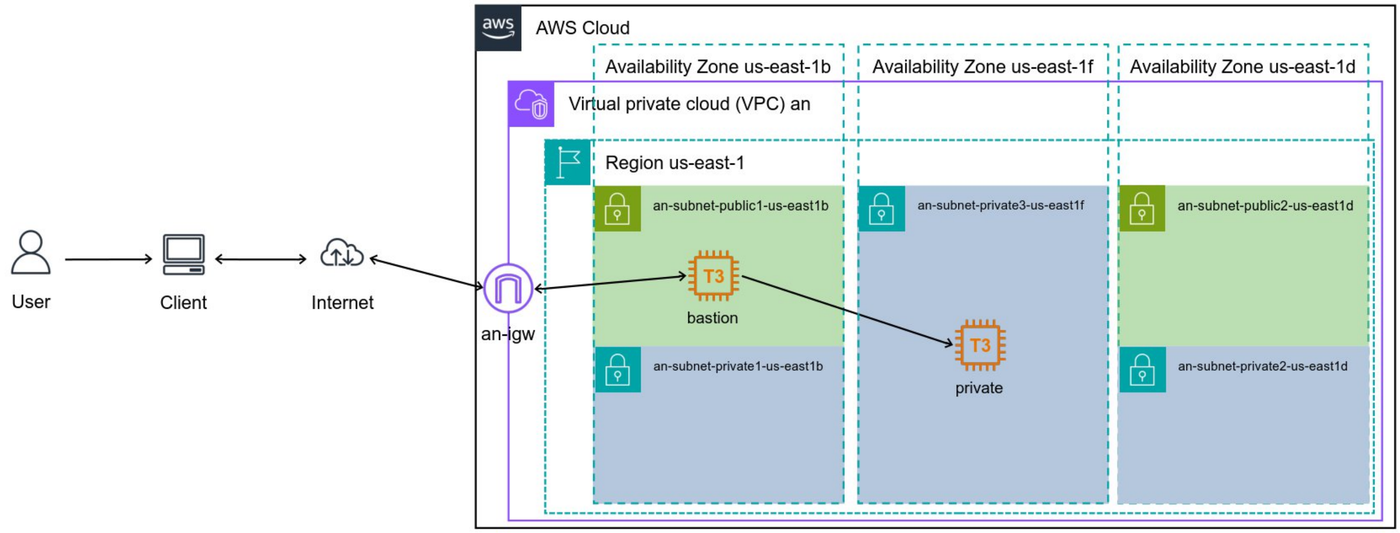
Just at the beginning of the current century, a seemingly [7] new concept arose and was just being explored: Virtual Private Network(s) [VPN]. Defined as "a network [...] [that] provides inter-connectivity to exchange information among various entities that belong to the VPN." [8], in other words, only members of said network could access the contents found within, having the characteristics of a private network, such as a close community of authorized users that would allow them to access various network-related *services* and *resources*.

Traffic originating and terminating within a VPN traverses only those *nodes* that belong to the private network. Also, traffic isolation prevents the disturbance of inner traffic to outer traffic, and vice versa. Having this in mind, perhaps the defining and selling point of a VPN it's found within the first components of its definition: *virtuality*, as this kind of network topology operate on top of preexisting shared physical network infrastructure.

To demonstrate an extension branch of the discussed technology, Amazon Virtual Private Cloud [VPC] [9] will be used in the following development in order to demonstrate resource isolation and access control within a same network, and what it could mean for threat handling and deescalation.

Diagram

The following architecture it's proposed as a graphic solution for the stated goals.


AWS Cloud
Availability Zone us-east-1b
Availability Zone us-east-1f
Availability Zone us-east-1d
Virtual private cloud (VPC) an
Region us-east-1
an-subnet-public1-us-east1b
an-subnet-private3-us-east1f
an-subnet-public2-us-east1d
User
Client
Internet
an-igw
T3
bastion
T3
private
an-subnet-private1-us-east1b
an-subnet-private2-us-east1d

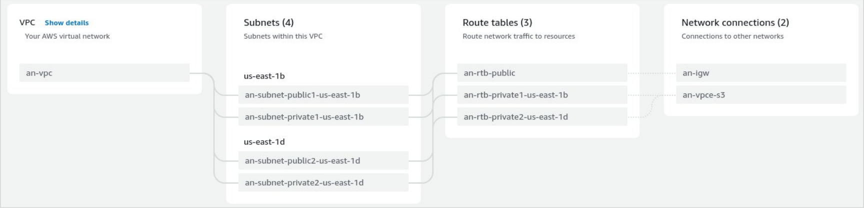
Practice Development

VPC Creation

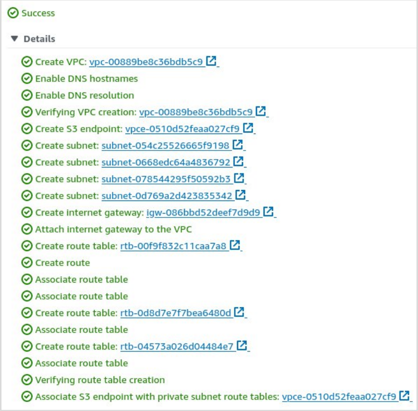
As in previous works, Amazon VPC has it's own dedicated dashboard inside the AWS console. Inside said section, a VPC it's created with the following features:

- Resources to create: VPC and more (network resources)
- Name: *an* (with auto-generate option enabled)
- IPv4 CIDR block: 10.0.0.0/16
- Tenancy: default
- Availability zones: 2
  - Custom picked us-east-1b and us-east-1d
- Public and private subnets: 2
- Custom CIDR blocks:
  - Public subnet b - 10.0.1.0/24
  - Public subnet d - 10.0.2.0/24
  - Private subnet b - 10.0.10.0/24
  - Private subnet d - 10.0.11.0/24
- No NAT gateways
- VPC endpoints: S3 Gateway
- DNS hostnames and resolution

The interface it's pretty straight forward, thus allowing anyone to create VPC's with relative ease with only these specifications. After the value all set, a diagram can be seen as a way of summarization of what is about to be created (result of *VPC and more* selection).


VPC
Show details
Your AWS virtual network
an-vpc
Subnets (4)
Subnets within this VPC
us-east-1b
an-subnet-public1-us-east-1b
an-subnet-private1-us-east-1b
us-east-1d
an-subnet-public2-us-east-1d
an-subnet-private2-us-east-1d
Route tables (3)
Route network traffic to resources
an-rtb-public
an-rtb-private1-us-east-1b
an-rtb-private2-us-east-1d
Network connections (2)
Connections to other networks
an-igw
an-vpce-s3

Each component can be selected to see the connection resolution path. As it can be seen, several routing tables are also provided, which will determine the set of rules that state how should packets will be forwarded through IP [10]. Having this configuration done, a screen confirming the success (or fail) at the VPC creation will be displayed.



✓ Success

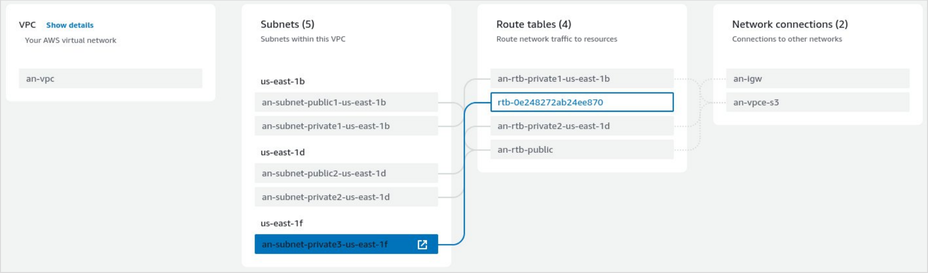
▼ Details

✓ Create VPC: vpc-00889be8c36bdb5c9
✓ Enable DNS hostnames
✓ Enable DNS resolution
✓ Verifying VPC creation: vpc-00889be8c36bdb5c9
✓ Create S3 endpoint: vpce-0510d52feaa027cf9
✓ Create subnet: subnet-054c25526665f9198
✓ Create subnet: subnet-0668edc64a4836792
✓ Create subnet: subnet-078544295f50592b3
✓ Create subnet: subnet-0d769a2d423835342
✓ Create internet gateway: igw-086bbd52deef7d9d9
✓ Attach internet gateway to the VPC
✓ Create route table: rtb-00f9f832c11caa7a8
✓ Create route
✓ Associate route table
✓ Associate route table
✓ Create route table: rtb-0d8d7e7f7bea6480d
✓ Associate route table
✓ Create route table: rtb-04573a026d04484e7
✓ Associate route table
✓ Verifying route table creation
✓ Associate S3 endpoint with private subnet route tables: vpce-0510d52feaa027cf9

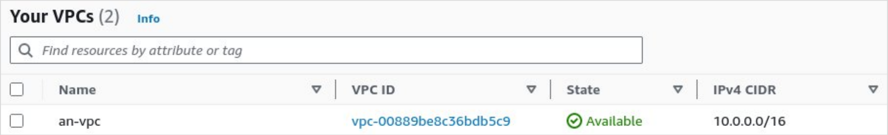
Having a successful creation, another private subnet has to be created within the same VPC; this can be achieved by accessing the “Subnets” section of the same panel. The details of this subnet are:

- Availability zone: us-east-1f (or any other that hasn’t already been selected)
- Custom CIDR block:
  - Private subnet f - 10.0.12.0/24

As this is a private subnet, it shouldn’t have access to the internet. This can be verified through the same diagram described before.


VPC
Show details
Your AWS virtual network
an-vpc
Subnets (5)
Subnets within this VPC
us-east-1b
an-subnet-public1-us-east-1b
an-subnet-private1-us-east-1b
us-east-1d
an-subnet-public2-us-east-1d
an-subnet-private2-us-east-1d
us-east-1f
an-subnet-private3-us-east-1f
Route tables (4)
Route network traffic to resources
an-rtb-private1-us-east-1b
rtb-0e248272ab24ee870
an-rtb-private2-us-east-1d
an-rtb-public
Network connections (2)
Connections to other networks
an-igw
an-vpce-s3

As noted, no internet gateway (igw) it’s shown for this new subnet, meaning that the configuration it’s correct. After both VPC configurations are made, it should be listed inside “Your VPCs” section.



Your VPCs (2) Info

Find resources by attribute or tag

☐	Name	VPC ID	State	IPv4 CIDR
☐	an-vpc	vpc-00889be8c36bdb5c9	✓ Available	10.0.0.0/16

Instance creation

Now, a couple of EC2 instances [11] will be created with these details:

Instance for public subnet B

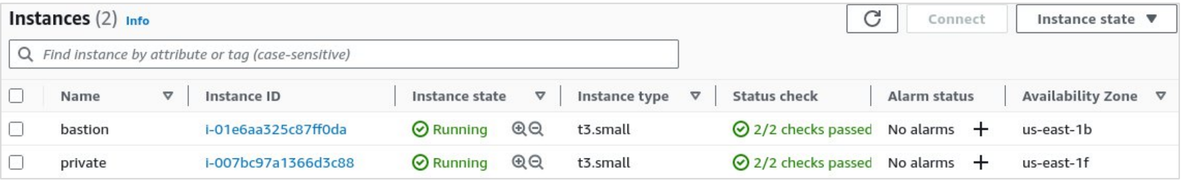
- Name: bastion
- OS: Windows Server (The latest available base version)
- Type: t3.small
- Key pair: vockey
- Network settings
  - VPC: an
  - Subnet: public subnet b
  - Auto-assign public IP
  - New security group with name *bastion*
- Small storage (around 30GB)

Instance for private subnet C

- Name: private
- OS: Windows Server (The latest available base version)

- Type: t3.small
- Key pair: vockey
- Network settings
    - VPC: an
    - Subnet: public subnet f
    - No auto-assign public IP (internet access prevention)
    - New security group with name *private*
    - Inbound security group rules
        - Type: rdp (for desktop access)
        - Source type: Custom
        - Source: bastion security group
- Small storage (around 30GB)

These instances should be listed, running, and status checked before RDP connection.



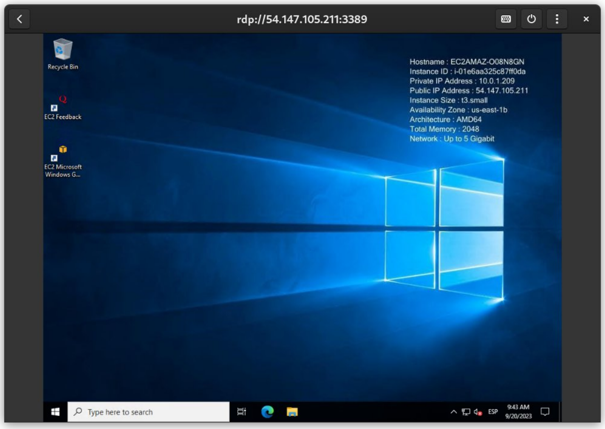
□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□	bastion	i-01e6aa325c87ff0da	✓ Running	t3.small	✓ 2/2 checks passed	No alarms +	us-east-1b
□	private	i-007bc97a1366d3c88	✓ Running	t3.small	✓ 2/2 checks passed	No alarms +	us-east-1f

Instance connection

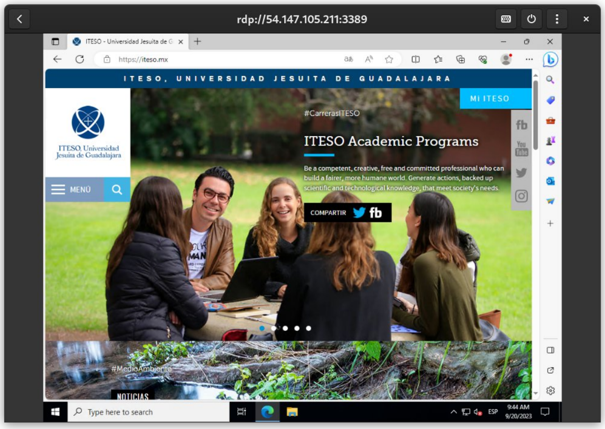
The final section of this development will conduct two tests: connection to both public and private instances.

Public instance

After password obtention, an RDP has to be used to connect to the first instance. *This should be possible*.



Hostname : EC2AMAZ-O08N8GN
Instance ID : i-01e6aa325c87ff0da
Private IP Address : 10.0.1.209
Public IP Address : 54.147.105.211
Instance Size : t3.small
Availability Zone : us-east-1b
Architecture : AMD64
Total Memory : 2048
Network : Up to 5 Gigabit

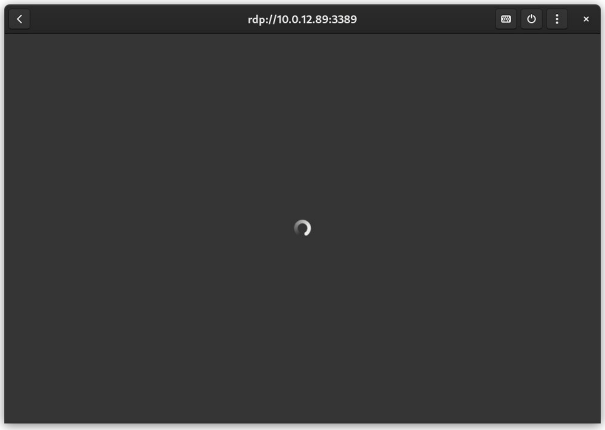


rdp://54.147.105.211:3389
ITESO - Universidad Jesuita de G
https://iteso.mx
ITESO, UNIVERSIDAD JESUITA DE GUADALAJARA
MI ITESO
ITESO Universidad Jesuita de Guadalajara
MENÚ
#CarrerasITESO
ITESO Academic Programs
Be a competent, creative, free and committed professional who can build a fairer, more humane world. Generate actions, backed up scientific and technological knowledge, that meet society's needs.
COMPARTIR
#MedioAmbiente
NOTICIAS
Type here to search
9:44 AM
9/20/2023

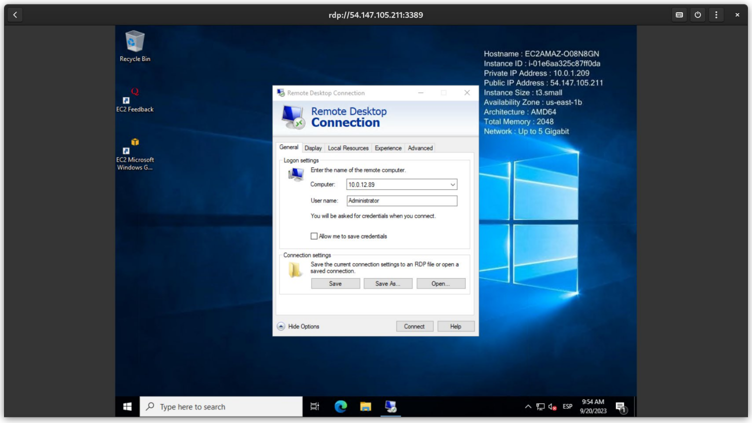
As it can be seen, RDP connection it's *indeed* possible, and also, the instance has internet access.

Private instance

Similar to the previous test, password obtention has to be made. An issue arises here, as no public IP is provided (on purpose). *RDP connection outside the VPC shouldn't be possible*.


rdp://10.0.12.89:3389

Once again, indeed, this native connection it's impossible, however, RDP it's still enabled, and a connection can be established within the previous instance.

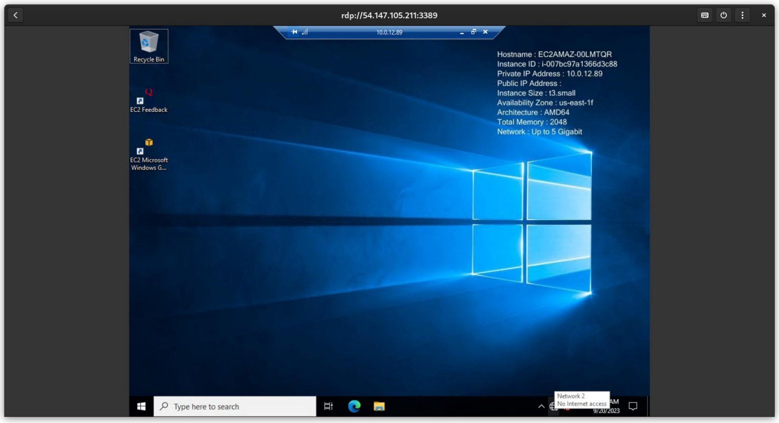

rdp://54.147.105.211:3389

Hostname : EC2AMAZ-O08N8GN
Instance ID : i-01e6aa325c87ff0da
Private IP Address : 10.0.1.209
Public IP Address : 54.147.105.211
Instance Size : t3.small
Availability Zone : us-east-1b
Architecture : AMD64
Total Memory : 2048
Network : Up to 5 Gigabit

Remote Desktop Connection

Logon settings
Enter the name of the remote computer.
Computer: 10.0.12.89
User name: Administrator
You will be asked for credentials when you connect.
□ Allow me to save credentials

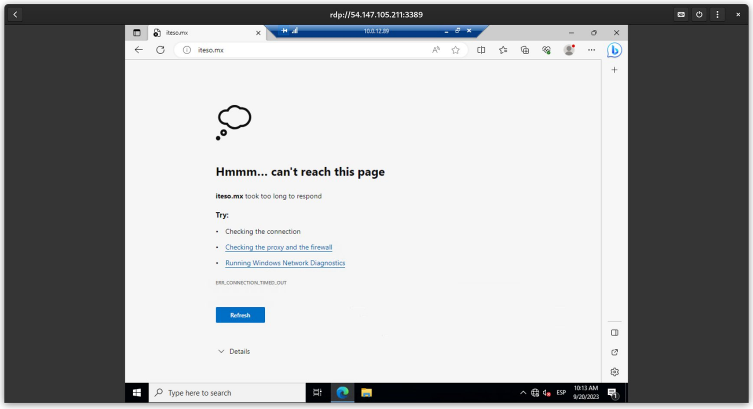
Connection settings
Save the current connection settings to an RDP file or open a saved connection.


rdp://54.147.105.211:3389

10.0.12.89

Hostname : EC2AMAZ-00LMTQR
Instance ID : i-007bc97a1366d3c88
Private IP Address : 10.0.12.89
Public IP Address :
Instance Size : t3.small
Availability Zone : us-east-1f
Architecture : AMD64
Total Memory : 2048
Network : Up to 5 Gigabit

Network 2
No Internet access


rdp://54.147.105.211:3389

10.0.12.89

iteso.mx

Hmmm... can't reach this page

iteso.mx took too long to respond

Try:

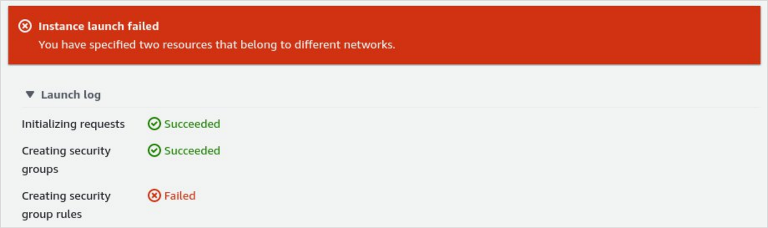
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

As demonstrated, the second instance can be accessed from the first one, but, as it was configured like this, internet access it's not available. This demonstration concludes the development.

Problems and Solutions

An interesting problem had to be solved, in which an instance couldn't be created because of a group rule issue.



Instance launch failed
You have specified two resources that belong to different networks.

▼ Launch log

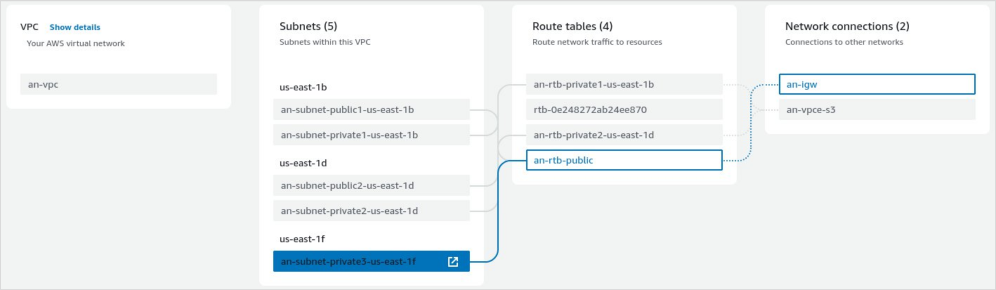
Initializing requests	✓ Succeeded
Creating security groups	✓ Succeeded
Creating security group rules	⊗ Failed

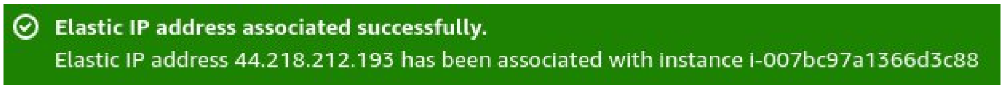
The root cause of this was that the second subnet was created inside a second VPC, an action that came from a misunderstanding of the material provided for this practice. The solution was rather simple, as the only thing that needed to be added was the mentioned subnet, but inside the unique VPC created.

Experiments and Results

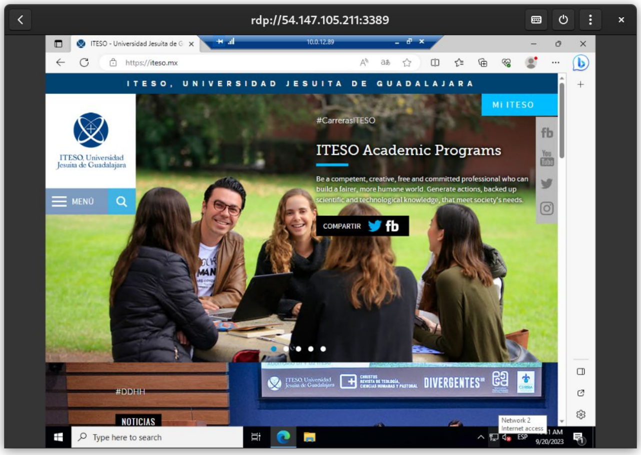
What if the second instance *did had* internet access?

To achieve this, the private subnet (1f) has to be associated with an internet gateway from the VPC section, and then, an elastic IP has to be associated to the private instance (this is omitted from the architecture diagram).

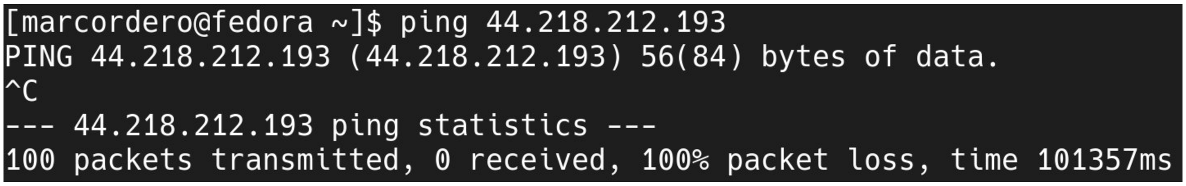

VPC Show details
Your AWS virtual network
an-vpc
Subnets (5)
Subnets within this VPC
us-east-1b
an-subnet-public1-us-east-1b
an-subnet-private1-us-east-1b
us-east-1d
an-subnet-public2-us-east-1d
an-subnet-private2-us-east-1d
us-east-1f
an-subnet-private3-us-east-1f
Route tables (4)
Route network traffic to resources
an-rtb-private1-us-east-1b
rtb-0e248272ab24ee870
an-rtb-private2-us-east-1d
an-rtb-public
Network connections (2)
Connections to other networks
an-igw
an-vpce-s3



Elastic IP address associated successfully.
Elastic IP address 44.218.212.193 has been associated with instance i-007bc97a1366d3c88


rdp://54.147.105.211:3389
ITESO - Universidad Jesuita de G
10.0.12.89
https://iteso.mx
ITESO, UNIVERSIDAD JESUITA DE GUADALAJARA
MI ITESO
ITESO Universidad Jesuita de Guadalajara
MENÚ
#CarrerasITESO
ITESO Academic Programs
Be a competent, creative, free and committed professional who can build a fairer, more humane world. Generate actions, backed up scientific and technological knowledge, that meet society's needs.
COMPARTIR
#DDHH
NOTICIAS
DIVERGENTES
Type here to search
Network 2 Internet access
ESP
9/20/2023

Now, the instance can have outbound traffic, but still remains inaccessible from outside the VPC.



```
[marcordero@fedora ~]$ ping 44.218.212.193
PING 44.218.212.193 (44.218.212.193) 56(84) bytes of data.
^C
--- 44.218.212.193 ping statistics ---
100 packets transmitted, 0 received, 100% packet loss, time 101357ms
```

This would be particularly useful for software updates, having to download certain files but remaining private.

Should local IPs be defined or have them auto assigned?

The short answer is that it depends.

On a more elaborated response, from time to time one would need a proof of concept, thus, requiring a quick solution for something that would be ephemeral, which, in that case, an IP address wouldn't need to be formally specified. Another scenario would be a previously defined network topology that would be migrated to cloud services, but heavily dependent on assigned or static IP's, such as CCTV systems and such.

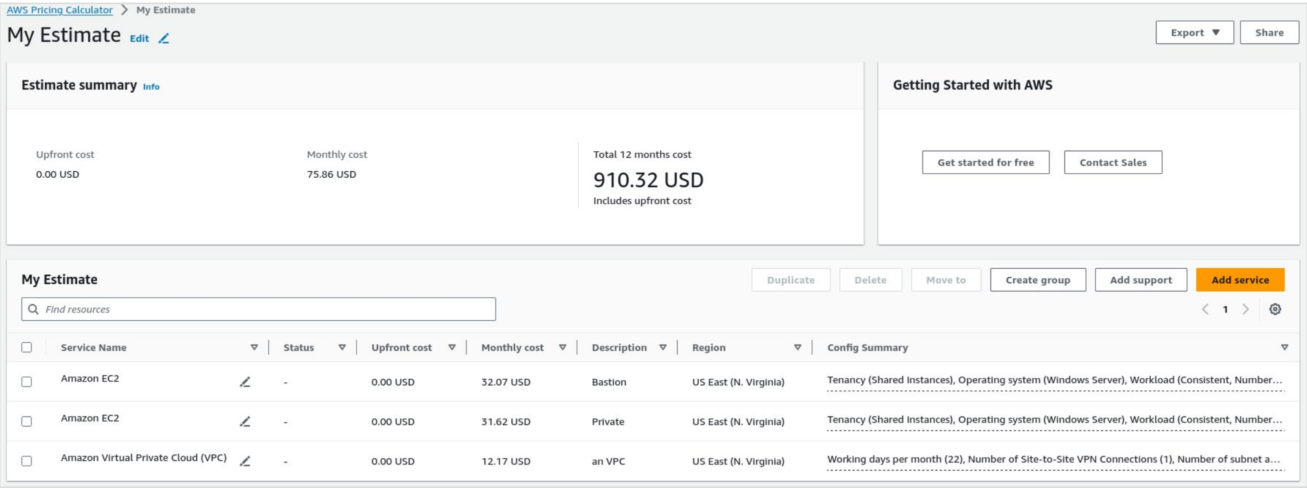
In the particular case of AWS, when linking an elastic IP address, one could specify where this address would be coming from, but the more common practice would be retrieving an address for Amazon own pool. This would be problematic, however, an static IP would still be provided.

Budget Justification

Taking into consideration:

- 2 similar EC2 instances
- A VPC with 5 subnets in the us-east-1 region

... With 100% utilization per month On-Demand for instances, the costs would be the following:



AWS Pricing Calculator > My Estimate

My Estimate

Estimate summary

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	75.86 USD	910.32 USD Includes upfront cost

Getting Started with AWS

My Estimate

	Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
□	Amazon EC2	-	0.00 USD	32.07 USD	Bastion	US East (N. Virginia)	Tenancy (Shared Instances), Operating system (Windows Server), Workload (Consistent, Number...
□	Amazon EC2	-	0.00 USD	31.62 USD	Private	US East (N. Virginia)	Tenancy (Shared Instances), Operating system (Windows Server), Workload (Consistent, Number...
□	Amazon Virtual Private Cloud (VPC)	-	0.00 USD	12.17 USD	an VPC	US East (N. Virginia)	Working days per month (22), Number of Site-to-Site VPN Connections (1), Number of subnet a...

Conclusions

The walkthrough of this practice has been something archaic in the sense that networking it's not something a lot of software (or computational systems in this case) engineers are often familiar with, however, it's always convenient to know at least a couple of underlying levels of knowledge about this concept. The thing is, even with very little and basic coverage of this area, the cloud used in this development makes it so easy to configure and deploy virtual networks that anyone could start to protect their project assets right away at creation steps.

The importance of this tools might not seem that relevant here and as of this point of progress, but when high risk data it's a stake, such as medical records, bank information, government documents, and similar content, configurations so easy to made and yet so easy to forget could be the inflexion point of the course of a business.

Bibliography

[1] Board of Regents of the University System of Georgia. 'A Brief History of the Internet'. [Online]. Available: https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml.

[2] IBM. 'IBM Mainframes'. [Online]. Available: https://www.ibm.com/ibm/history/exhibits/mainframe/mainframe_intro.html.

[3] Airfocus. 'Software Feature'. [Online]. Available: https://airfocus.com/glossary/what-is-software-feature/.

[4] Scos Training. 'History of TCP/IP'. [Online]. Available: https://scos.training/history-of-tcp-ip/.

[5] J. Firch. ' Common Types Of Network Security Vulnerabilities'. [Online]. Available: https://purplesec.us/common-network-vulnerabilities/.

[6] S. Borg Psaila. ''UN declares Internet access a human right' – did it really?'. [Online]. Available: https://www.diplomacy.edu/blog/un-declares-internet-access-human-right-did-it-really/.

[7] A. S. Gillis, 'VPN (virtual private network)'. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/virtual-private-network.

[8] R. Venkateswaran, "Virtual private networks," in IEEE Potentials, vol. 20, no. 1, pp. 11-15, Feb-March 2001, doi: 10.1109/45.913204.

[9] Aws.amazon.com, 'What is Amazon VPC'. [Online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html.

[10] K. Yasar. 'routing table'. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/routing-table.

[11] Aws.amazon.com, 'Amazon EC2'. [Online]. Available: https://aws.amazon.com/es/ec2/.