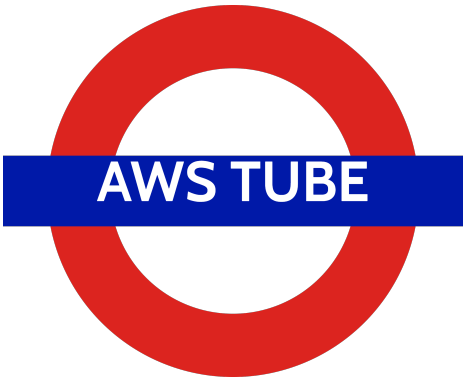

Figure 1: CLICK HERE TO RETURN TO STATION

Recovery Sheet 4

SJ Green

Recovering from the session delivered on the night of Wednesday 5th February 2025. This is the second session on AWS Networking. You can view the recovery sheet for the previous week here. Take your time with this sheet. It is designed to allow you to grade your approach. Start with the Active-Active section. Repeat it a few time if you are really confused. Then, you can take things a step further with the Warm Standy section, and so on. As a revision exercise, you could learn the definitions of the Active-Active sections, across all the weeks. Once you feel you have mastered this sheet, start preparing with Recovery Sheet 5, where we think about computing on AWS.

1 Active-Active

Description

1. **Internet Gateway (IGW)** A construct which allows resources inside your VPC (network, essentially) to communicate with the Internet. The Internet Gateway goes in the walls of the VPC, on schematic diagrams. It does not go in the walls of subnets, and that's important.

   You'll see the word GATEWAY used in lots of AWS products such as

Amazon API Gateway, AWS Storage Gateway and you also have the NAT Gateway construct (which exists in the VPC product). Generally, a gateway is a device or node that connects two disparate networks. The term has a long history: Bill Cheswick wrote a paper in 1990, for example, called *The Design of a Secure Internet Gateway*. Bill Cheswick worked on firewalls... you'll notice that the word **GATEWAY** has connotations of gates, and *restriction* of access. To allow resources to send traffic to the Internet, you change the route table that is associated with the subnet holding the resource. Recall that routes consist of targets and destinations. The target (**tangible** thing to aim for) should be the IGW ID, and the destination is conventially the CIDR range 0.0.0.0/0.

2. **NAT Gateway** NAT stands for Network Address Translation. This is a construct that allows resources in your subnet to have their IP addresses (their network addresses, that is) **translated**. The NAT Gateway is thus like the scrupulous editor of a newspaper article who swaps out the real names of the whisteblowers for a fake name.

   In fact, this attempted analogy forces us to clarify things. Whisteblowers, and those speaking on the evening TV news with blurred faces, have their names "translated" in order to keep their identities secret. The concern is the security of the person. It is true that the concern amongst VPC admins, when they use a NAT Gateway, can be the **security** of their resource. If you use a NAT Gateway, then a resource can communcate with the Internet without having a public IP address. (Giving things public IP addresses is disadvantageous because then it is exposed to the Internet and people have an attack surface to aim at.) "Can't someone just aim traffic at the attack surface which is the NAT Gatway?". Well, yes, they can try. However, NAT Gateways "cannot receive unsolicited connection requests" (VPC User Guide). With a NAT Gateway, EC2 Instances in private subnets can send outbound traffic to the Internet. Recall that a *private subnet* is nothing but a subnet with no route to the Internet in its associated route table. If using a NAT Gateway for this, the NAT Gateway **goes in a public subnet**, and you add a route to the subnet housing your resource. The route allows the private resource to send traffic to the public subnet (from the private subnet). The public subnet has a route to the Internet Gateway (which is attached to no particular subnet, but rather the *VPC*).

   So, translation is important for security, and the security of people's well-being. Think, for example, about how emergency services translate vivid descriptions into cold and clinical codes, partly in order to avoid alarming the general public, and why dialects and slang develops. Translation has other uses besides security, though. It can **mould and simplify**. There are some classic examples of this; *eros*, *philia* and *agape* get simplified to "love" while *tu* and *usted* get simplified to "you". NAT Gateways can sim-

plify too. "You can use a **private** NAT Gateway to enable communication from your VPCs to your on-premises network using a pool of allow-listed addresses. Instead of assigning each instance a separate IP address from the allow-listed IP address range, you can route traffic from the subnet that is destined for the on-premises network **through a NAT Gateway** with an IP address from the allow-listed range". (VPC User Guide 2025). You can also use NAT Gateways to enable communication between overlapping networks. Sometimes networks have overlapping CIDR ranges. This solution does also involve a Transit Gateway and an ALB (which we'll meet later) but know that it's possible to route traffic between VPCs using a private NAT Gateway (VPC User Guide).

3. **Security Groups (SG)** are firewalls that control which traffic can go to and from an ENI (Elastic Network Interface). EC2 Instances communicate using Elastic Network Interfaces so you can use Security Groups to protect your EC2 Instances. SGs protect other entities too, such as Application Load Balancers. SGs do not have Allow rules and Deny rules. They only have Allow rules. Each rule consists of a **Type** field, **Protocol**, **Port**, **Source** and **Description** (see Jeff Barr 2017). The Protocol field tends to be Transmission Control Protocol (TCP) which operates at Layer 4, the Transport Layer.
4. **NACL** Description.
5. **AWS Network Firewall** Description.
6. **AWS Global Accelerator** Description.
7. **Elastic Network Interface (ENI)** Description
8. **Elastic Network Adapter (ENA)** Description
9. **Elastic Fabric Adapter (EFA)** Description
10. **High Performance Computing (HPC)** Description

2 Warm Standby

1. **Internet Gateway (IGW)** Description
2. **NAT Gateway** Description
3. **Security Group (SG)** Description.
4. **NACL** Description.
5. **AWS Network Firewall** Description.

6. **AWS Global Accelerator** Description.
7. **Elastic Network Interface (ENI)** Description
8. **Elastic Network Adapter (ENA)** Description
9. **Elastic Fabric Adapter (EFA)** Description
10. **High Performance Computing (HPC)** Description

3 Pilot Light

The pilot comes aboard ships in unfamiliar waters to sort out shit.

1. **Internet Gateway (IGW)** Description
2. **NAT Gateway** Description
3. **Security Group (SG)** Description.
4. **NACL** Description.
5. **AWS Network Firewall** Description.
6. **AWS Global Accelerator** Description.
7. **Elastic Network Interface (ENI)** Description
8. **Elastic Network Adapter (ENA)** Description
9. **Elastic Fabric Adapter (EFA)** Description
10. **High Performance Computing (HPC)** Description

4 Backup

1. **Internet Gateway (IGW)** Description AWS Removes NAT Gateway's Dependence on Internet Gateway. Available at: `https://www.reddit.com/r/aws/comments/nxj7gf/aws_removes_nat_gateways_dependence_on_internet/?rdt=63484`
2. **NAT Gateway** Description

   Green, Sam (2025). Implementing a NAT Gateway. Available at: `https://www.youtube.com/playlist?list=PLn2pda68RIHUsfMS790VWaMp8UF2TW3hu`

   This is a playlist of videos on YouTube. It shows me implementing an NAT Gateway, predominantly using the AWS CLI.
3. **Security Group (SG)** Description.

4. **NACL** Description.
5. **AWS Network Firewall** Description.
6. **AWS Global Accelerator** Description.
7. **Elastic Network Interface (ENI)** Description
8. **Elastic Network Adapter (ENA)** Description
9. **Elastic Fabric Adapter (EFA)** Description
10. **High Performance Computing (HPC)** Description