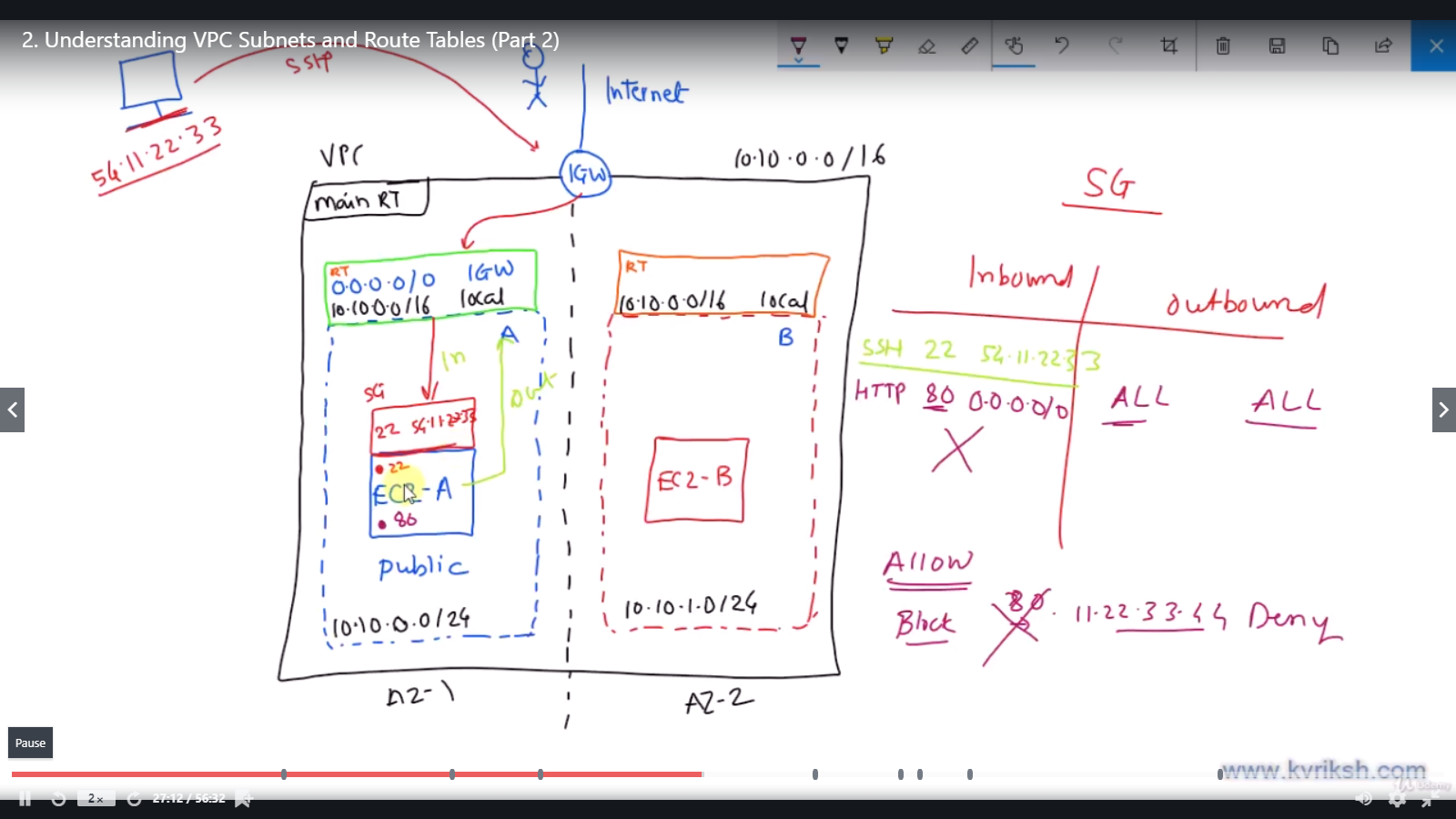
**Firewall:**

**Security Group**



**Brian Dump:**

* Security group acts as a virtual firewall ; first level of defence
* Default : it allows no inbound and allows all outbounds
* You can not add entry to deny any ip’s
* ONLY you can add entries to allow the inbound.
* Security group is separate entity which means one security group can be associated with multiple instances

It has two elements

* **Inbound**
  + By default, inbound table is empty which means security group will not allow outside world to connect with the device
  + We can only add the entries to enable particular ip/ ip rage & ports
* **Outbound**
  + By default , the outbould table is empty and set to allow all traffic going out.

**Network Access Control Lists:**

NACL stands for Network Access Control Lists. It is a security layer for your VPC that controls the traffic in and out of one or more subnets.

You can set up a Network ACL similar to the security group that adds an additional layer of security to your VPC.

* By default, allows all inbound and outbound
* If you want to block any ip, we can do it in NACL
* If you allow any ip in inbound, then we have to add entry in outbound as well

Apply NACL - if you want to add rules to the entire Subnet.

Apply Security group - if you want rules specific to Instances

