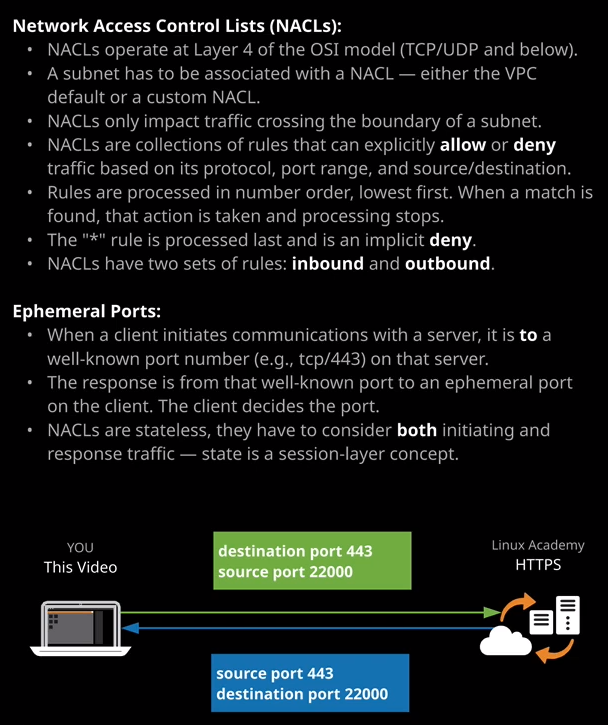
**Network access control lists also know as NACLs**

**Network ACLs are a security feature inside AWS VPCs and they're associated with one or more subnets. A subnet can only be associated with a single NACL. A VPC, when you create it, is created with the default NACL. If subnets inside that VPC aren't specifically associated with a NACL that you've created, then they're associated with this default network ACL for the VPC.**



Now **network ACLs control data traffic, which crosses a subnet.** So this means that if you've got communication occurring between two instances inside a subnet, they won't be impacted by the network ACL that surrounds that subnet. That's critical to understand for the exam. Only traffic which crosses the boundary of a subnet— so traffic that leaves to go to another subnet, traffic that leaves to reach the internet, traffic that's coming in from the internet or entering from another subnet only those types of traffic are impacted by a network ACL. For anything that occurs inside a subnet that is not impacted by a network ACL.

**Now NACL is actually container for two sets of rules.** If I go to the VPC console and I open the default network ACL for one of our VPCs so I'm going to scroll down to Network ACLs. I'm going to look specifically at the one for the VPC that I've just created for VPC demo a Network ACL has two sets of rules **inbound rules and outbound rules**. **The inbound rules apply to traffic, which is entering a subnet, which this NACL is associated with. The outbound rules impact traffic, which is leaving a subnet that this network ACL is associated with.** Again any traffic or any communications between things inside the subnet that is not impacted by a network ACL.

Now every rule inside a network ACL has a rule number. This is an example rule number 100 and the rules are processed based on this number, it's a prioritized system. **So any rules with a lower rule number are higher priority. So the higher the rule number goes, the lower the processing priority.** Remember that one, it's important. In every network ACL we've always got this rule on both inbound and outbound. It's the one that's identified by this star as the rule number, and this is a default deny rule. If no other rules match inside this inbound or outbound rule set for a given network ACL then this rule, which is to deny that traffic is always applied.

The way that network ACLs work is that when traffic enters or leaves a subnet each rule in the appropriate rule set. So if it's inbound traffic, it's inbound. If it's outbound traffic, it's outbound but wherever the direction, each of the rules are processed one by one until one of them matches and when it matches, depending on the allow or deny that traffic is either allowed or denied but once that rule has finished processing, once traffic has been allowed or denied processing stops for that particular packet that's going through the subnet. That's why the order matters. So if you've got a rule that's going to lower rule number, say rule number 80 and that's processed it matches and say that it allows traffic then nothing else in the NACL processes. So it doesn't matter if you've got a rule number, say rule number 100 which allows traffic if you've got a lower rule number that denies it and that traffic is going to be denied and vice versa. **So the rule number inside network ACLs really does matter. You need to remember that for the exam, things are processed first with lower rule numbers, and then it continues processing until it gets a match.**

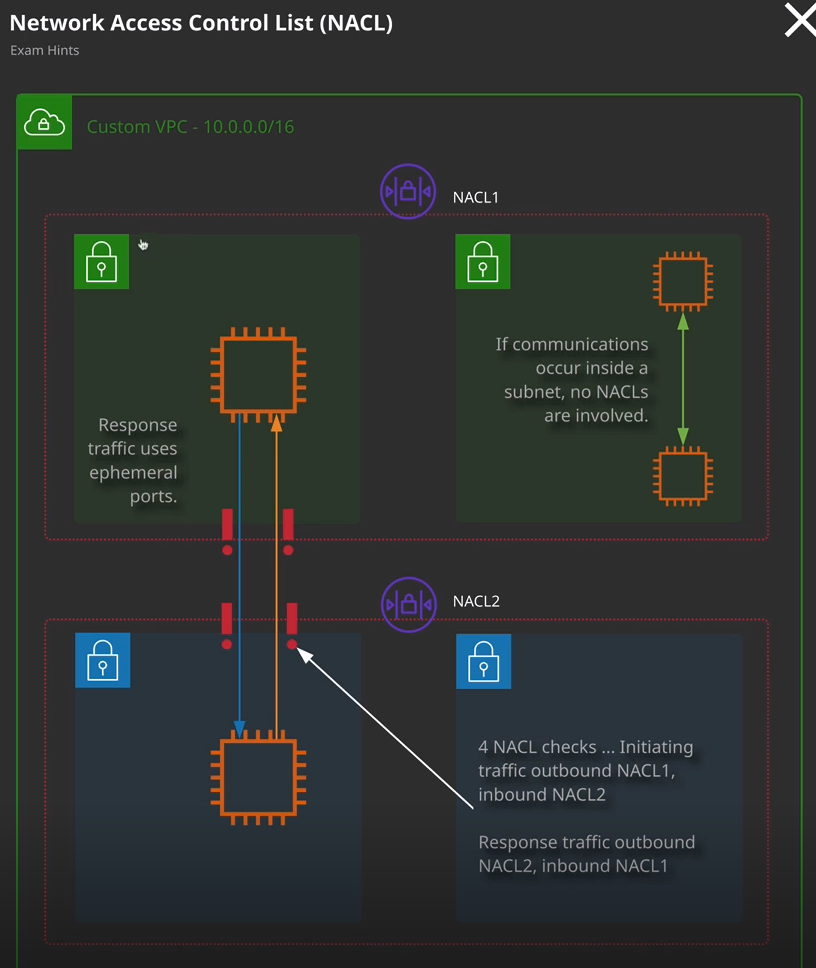
Now for the default network ACL the one that's created when you make a VPC, there's this implicit deny so this blocks or denies any traffic that isn't matched by another rule but you've also got this standard rule of 100 that's present on the inbound rules and the outbound rules, and this allows all traffic. Now, the effect of this is that these network ACLs the ones that are created with the VPC they allow all traffic, they essentially have no effect, and the reason for that is that network ACLs are a lot harder to manage than security groups and so, by default they don't apply to these default VPCs that get created either when you make the account or when you go to create the default VPC. So remember **that the default network ACL that gets created with every VPC while it does have this default implicit deny that blocks everything. It also has a rule number 100 that allows everything so in effect, it doesn't block any traffic.** Now this is only the case for network ACLs created with the VPC.

If you create a network ACL manually, let's say I create this one and I call it newnetworkACL or NACL and I associate it with VPC demo. If a hit Create and then look at the rules were created on this one, this doesn't have that rule number 100. **So the default for any network ACLs that you create is that everything is denied.**

Now it's important that you understand the structure of these rules, so inbound rules apply to incoming traffic. Outbound rules apply to outgoing traffic but for every rule we've got a number of columns. The first is we got the traffic type so you can specify a particular type of traffic. Maybe it's pop3, IMAP, HTTPS, or even a custom type, maybe all TCP, all UDP, or even all traffic. So if you select a custom TCP rule, so you want to act on a certain type of TCP traffic, then the protocol selected. You'll need to specify a port or a port range and then a source IP address and then, whether you want to allow or deny that traffic, you can select a custom protocol rule and then select a specific layer four or layer three protocol but in general, what you going to be doing with these rules is allowing or denying specific types of traffic. So TCP, UDP, ICMP, or a particular grouping. Now **the important thing to understand about network ACL rules is that you can only allow or deny traffic based on the protocol, the port or port range, the IP address, or an IP address range so a CIDR and for that grouping, you can allow or deny traffic what you can't do like you can do with a security group is reference logical resources. Network ACLs are layer four or below construct. You can only reference IPs, CIDRs, protocols, and port ranges. You cannot reference logical AWS resources because network ACLs are only applied to subnets.**

You can't have these applied directly to things like EC2 instances. They only apply when traffic from resources crosses the subnet boundary. Now what you can do with network ACLs which you can't do with security groups, is to explicitly deny things. So with security groups, you're actually allowing traffic to flow through them but you can't explicitly deny things. Now take this as an example. Let's say that you've allowed a network range to connect your website. Maybe it's a network of a partner or a vendor and you wanting them to connect your website. So you make a security group, and you allow their IP range to connect your web server but what if one of their machines becomes infected with malware and you want to restrict that you want to deny it well you can't do that with a security group. With the network ACL you could allow their entire network range and that's one rule, but then have a deny rule with a lower rule number. Remember, the order is important, so you have a deny rule with lower rule number it's process first, it's for a specific IP. It's set to deny and that blocks that particular infected machine from accessing your website. **So network ACLs have specific advantages in that they do allow these explicit denies,** and that's important to understand for the exam, Network ACLs operate at layer four of the seven layer network model. Now this has an important limitation.

When you're communicating with a server, let's say you're watching this video on your laptop right now and you're communicating with Linux Academy web server. From a layer four point of view what you're doing if you're establishing an initiating connection with the web server and the destination of this is on port 443. So this is a known used port. This is HTTPS. You're connecting from a port on your local machine and you're connecting to the Linux Academy server but what's also happening is the server is responding to this initiating connection with an inbound connection back to you. This is known as the response connection or the reply connection. Now this is from this well known port so port 443 and it connects to a port on your local machine known as an ephemeral port. It's a short lived port. You specify this port. So when you create this outgoing connection, you tell it the port that you want it to be connected back to on the server does that. Now, if you look at these two connections there actually part of the same conversation but from a layer four perspective, there isn't the concept of conversations or sessions. It's two independent connections. Now what this means is you need to handle both the outbound initiating connection and the inbound connection. They're part of the same thing**. So NACLs are what's known a stateless. They don't understand sessions. They don't understand that these two connections a part of the same conversation. With security groups, if you allow an incoming connection to your web server, you automatically allow the return traffic because security groups do understand sessions. They understand layer five of the OSI model. So security groups are much easier to administer then NACLs because with NACLs, every conversation to a thing is actually an outbound and an inbound connection, and you need to remember both of those.** You need to allow inbound on port 443 as well as outbound on a wide range of ports that are known as ephemeral ports and I'll make sure I include a link in the lesson description, which details these ephemeral ports and how you use them in network ACLs. Now, why this matters is because it can get fairly complicated.



If you have two instances that are communicating across two different subnets and you have each of those subnets surrounded by a different network ACL. So in this case, we've got an instance in this subnet and an instance in this subnet. Now this subnet is affected by NACL one. This one is affected by NACL two. Now, because it doesn't support sessions because it's not aware of conversations. We now know that when this instance talks to this instance, there's an outbound initiating communication and a return communication. What this means, though, is that this outbound communication first it exits this subnet, so it's affected by the outbound rule on NACL one. Then it enters this subnet so it's affected by the inbound rule on NACL two then, this instance responds to this instance and that is affected by the outbound rule set on NACL two and the inbound rule set a NACL one. **Now that means that for a single communication, you might have to worry about four individual rules so an outbound and an inbound on one NACL and an outbound and inbound on another NACL and if you also want to allow true return communications, so you want this instance to be able to initiate communications back to this instance as a separate communication, you need to do all of the same in reverse.** Now you don't need to know this level of complexity for the associate exam it's something that will come up in the networking specialty exam but I want you to be aware of it because it's why NACLs tend not to be used all that much. **Generally in production usage I try to make use where possible of security groups. I only use NACLs when I need to explicitly deny traffic. That's where their power comes from when you want to explicitly block one IP address or a whole network then NACLs allow you to do that where security groups don't. So NACLs operate at layer four of the OSI model, security groups operate at layer five, and that's why they understand that a single communication stream is initiation, traffic, and response.**