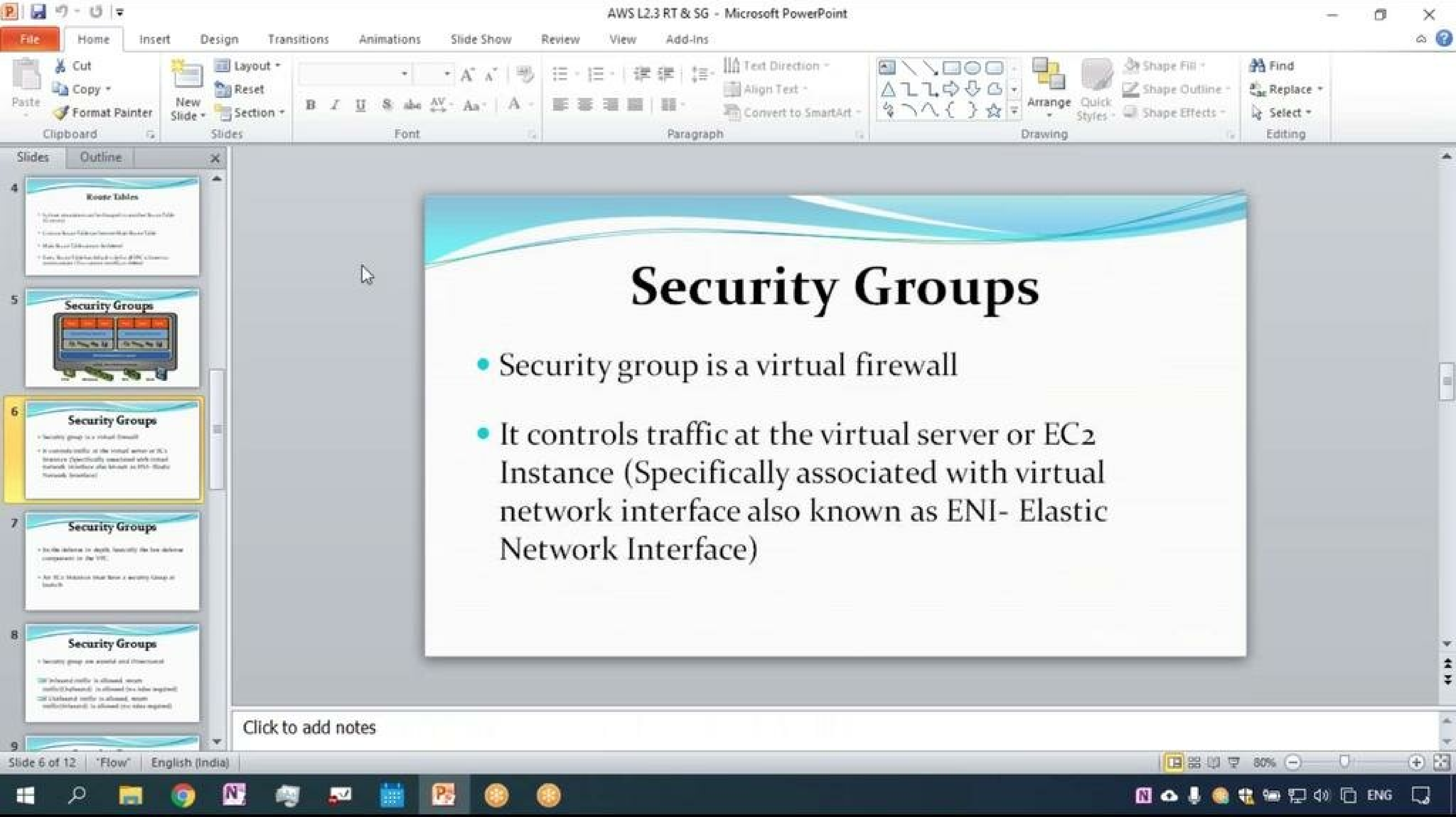
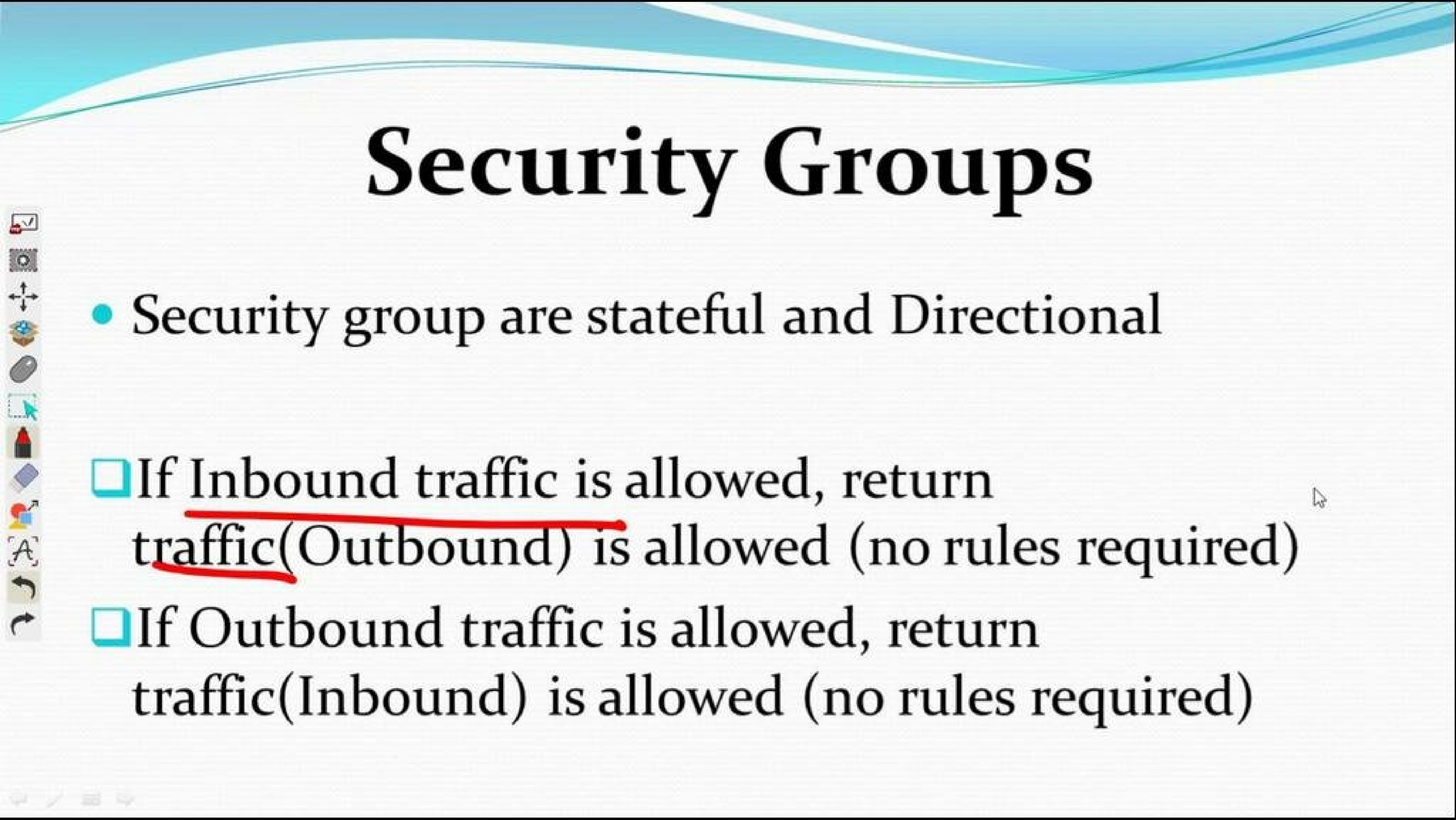


Security Groups

- Security group is a virtual firewall
- It controls traffic at the virtual server or EC2 Instance (Specifically associated with virtual network interface also known as ENI- Elastic Network Interface)

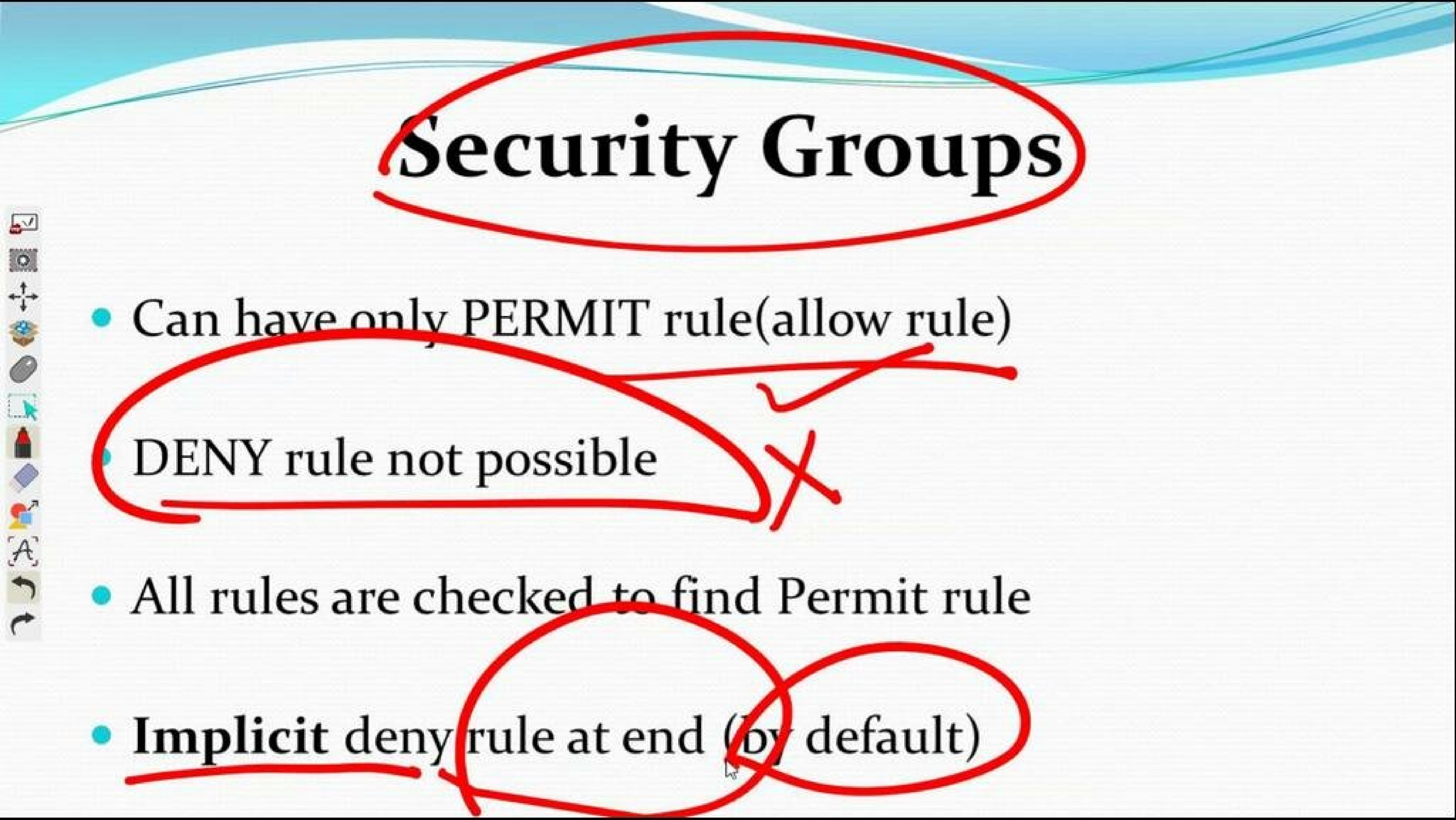


Security Groups

- Security group are stateful and Directional

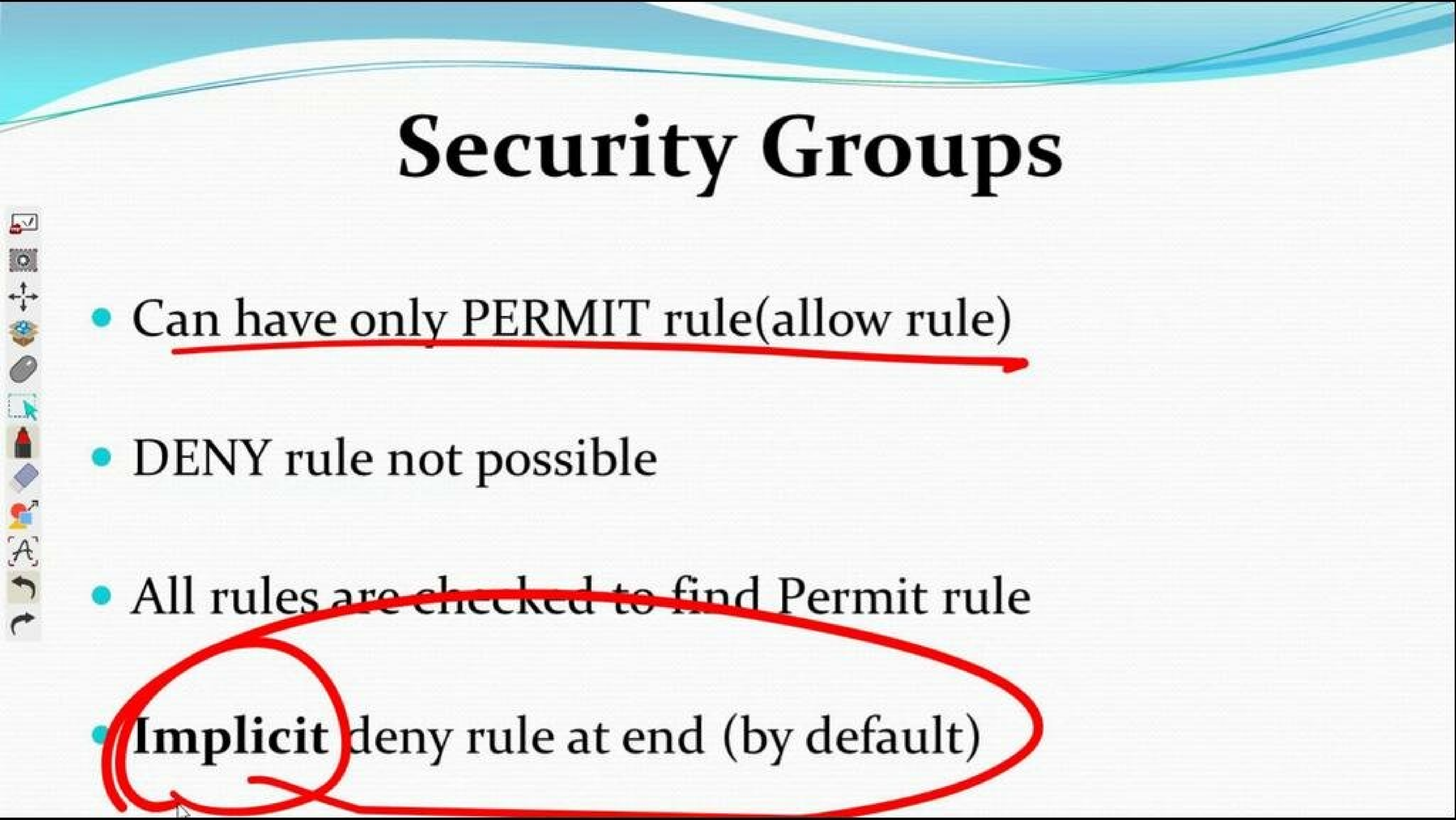
□ If Inbound traffic is allowed, return traffic(Outbound) is allowed (no rules required)

□ If Outbound traffic is allowed, return traffic(Inbound) is allowed (no rules required)



Security Groups

- Can have only PERMIT rule(allow rule) ✓
- DENY rule not possible ✗
- All rules are checked to find Permit rule
- **Implicit** deny rule at end (by default)

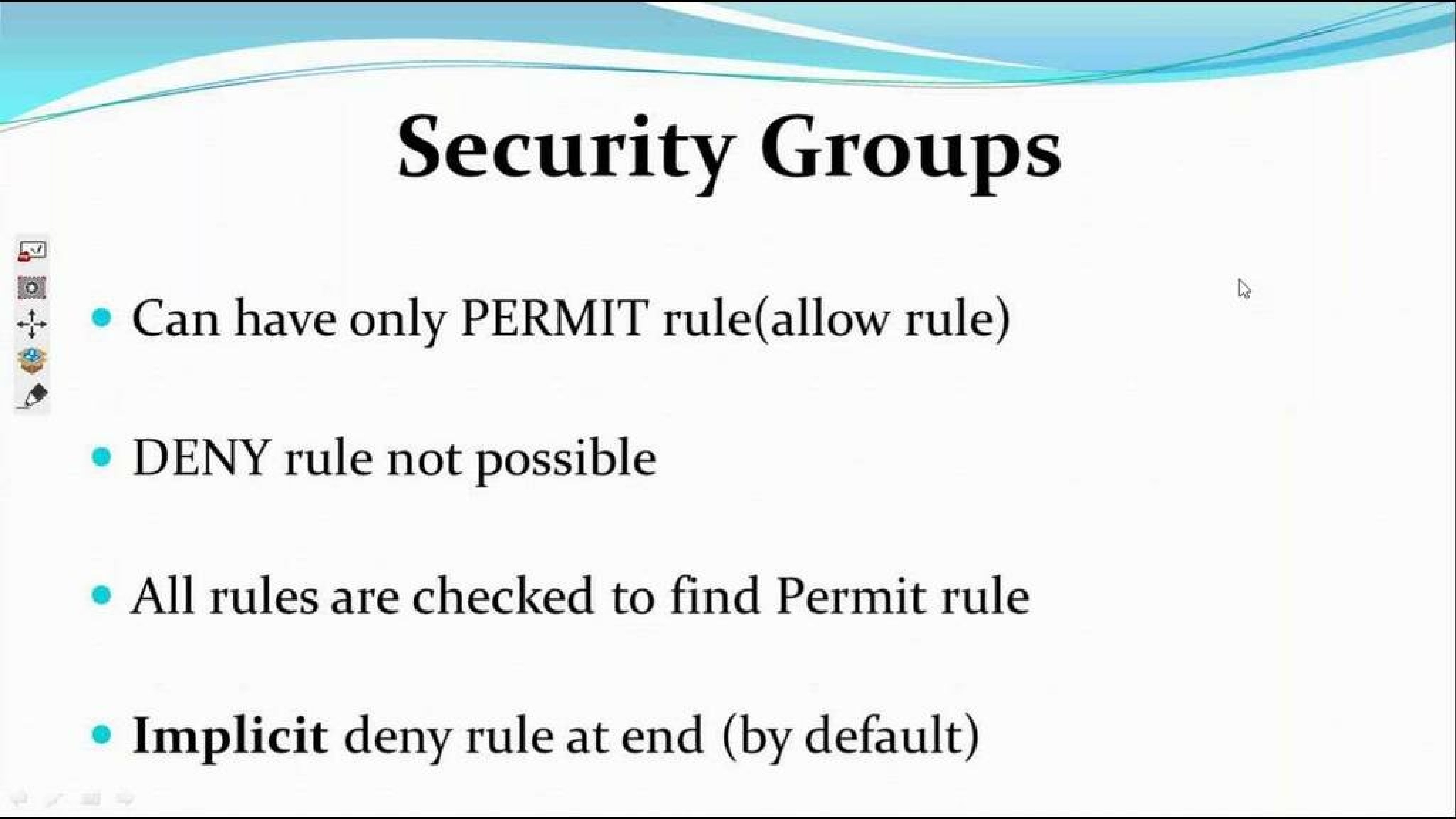


Security Groups

- Can have only PERMIT rule(allow rule)
- DENY rule not possible
- All rules are checked to find Permit rule
- **Implicit** deny rule at end (by default)

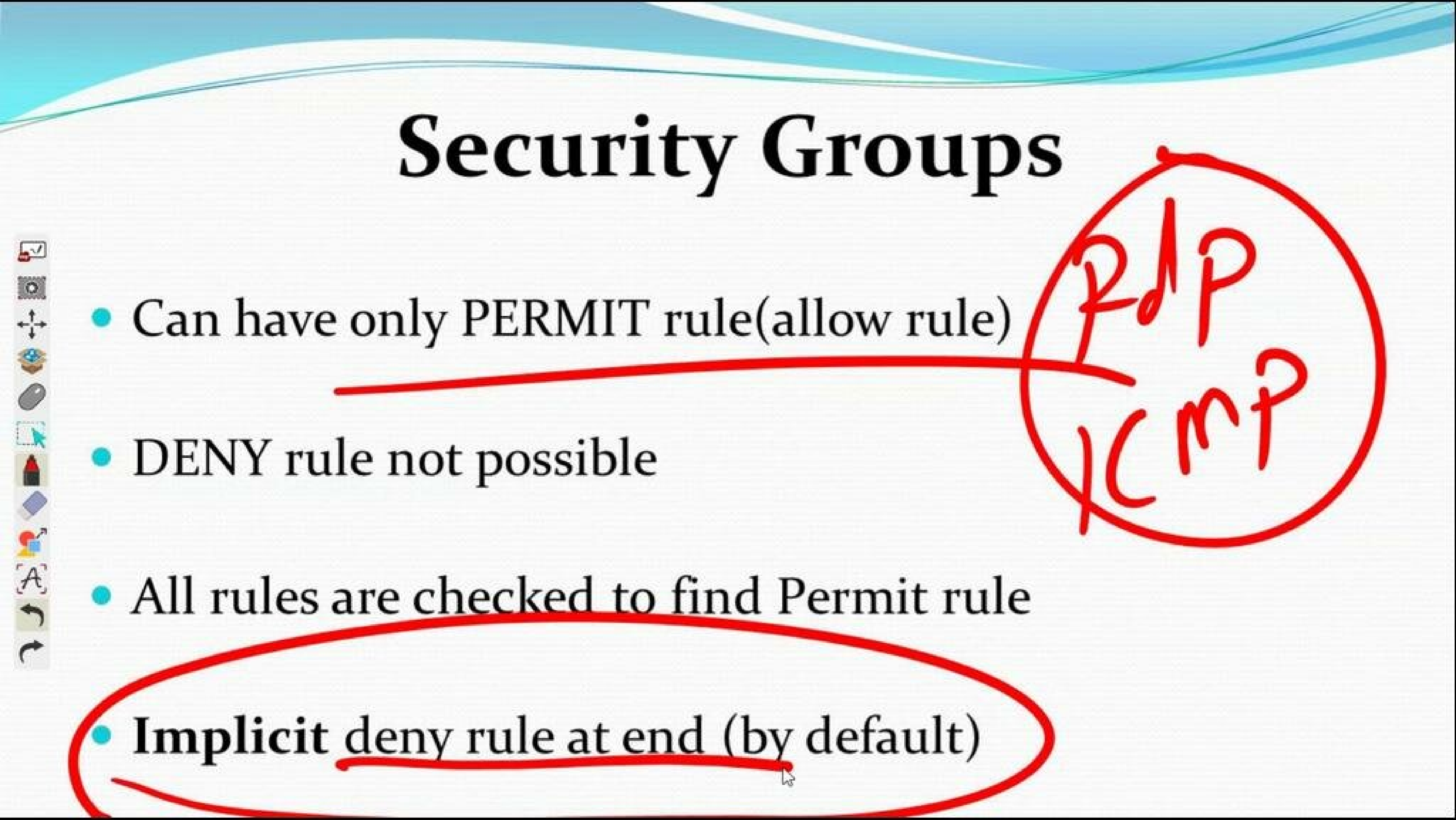
Security Groups

- Can have only PERMIT rule(allow rule)
- DENY rule not possible
- All rules are checked to find Permit rule
- **Implicit** deny rule at end (by default)



Security Groups

- Can have only PERMIT rule(allow rule)
- DENY rule not possible
- All rules are checked to find Permit rule
- **Implicit** deny rule at end (by default)



Security Groups

- Can have only PERMIT rule(allow rule)
- DENY rule not possible
- All rules are checked to find Permit rule
- **Implicit** deny rule at end (by default)

RDP
ICMP

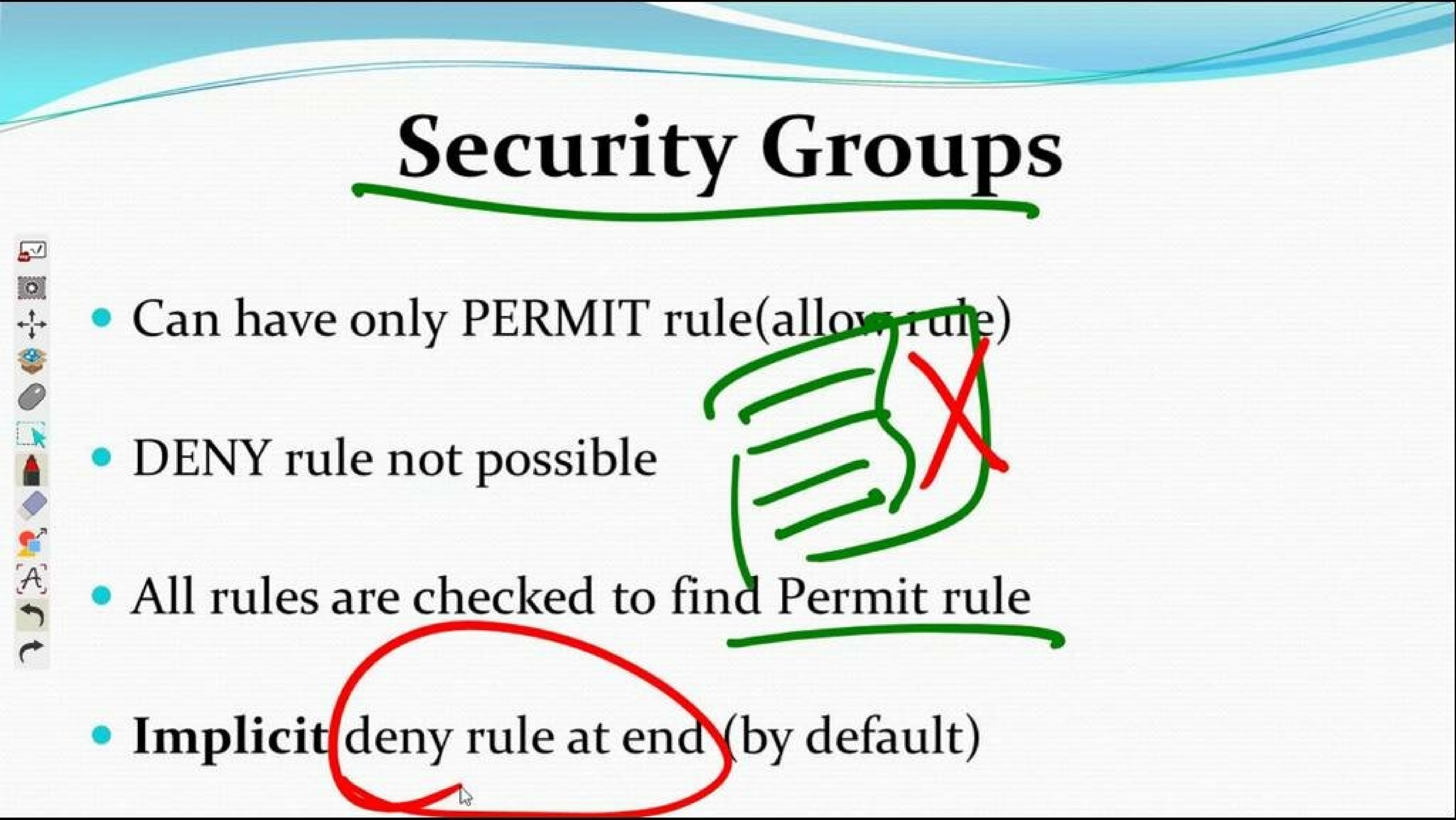
tu Rule

Security Groups

- Can have only PERMIT rule(allow rule)
- DENY rule not possible

NACL

- All rules are checked to find Permit rule
- **Implicit** deny rule at end (by default)



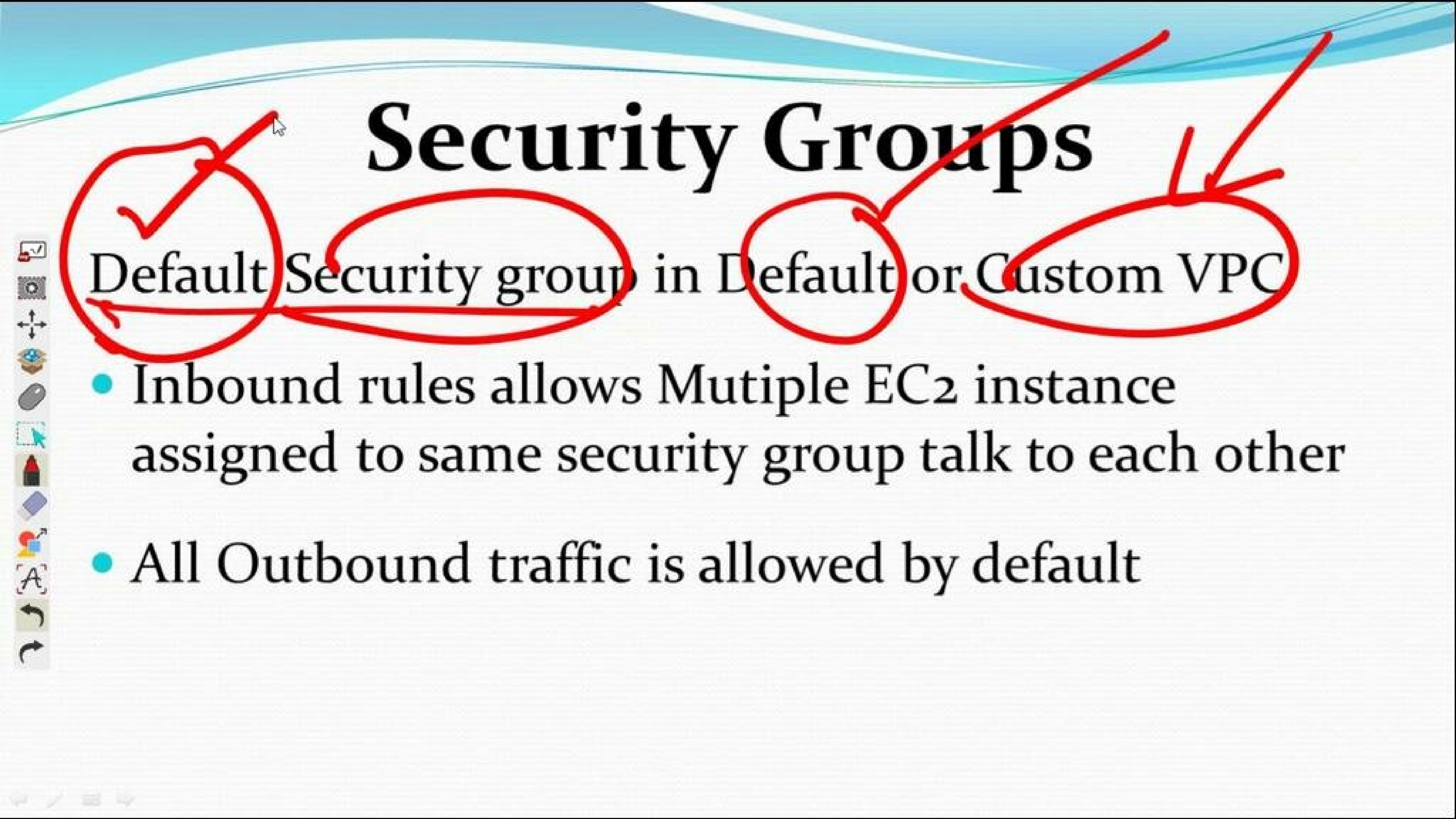
Security Groups

- Can have only PERMIT rule(allow rule)
- DENY rule not possible
- All rules are checked to find Permit rule
- **Implicit** deny rule at end (by default)

Security Groups

Default Security group in Default or Custom VPC

- Inbound rules allows Mutiple EC2 instance assigned to same security group talk to each other
- All Outbound traffic is allowed by default



Security Groups

Default Security group in Default or Custom VPC

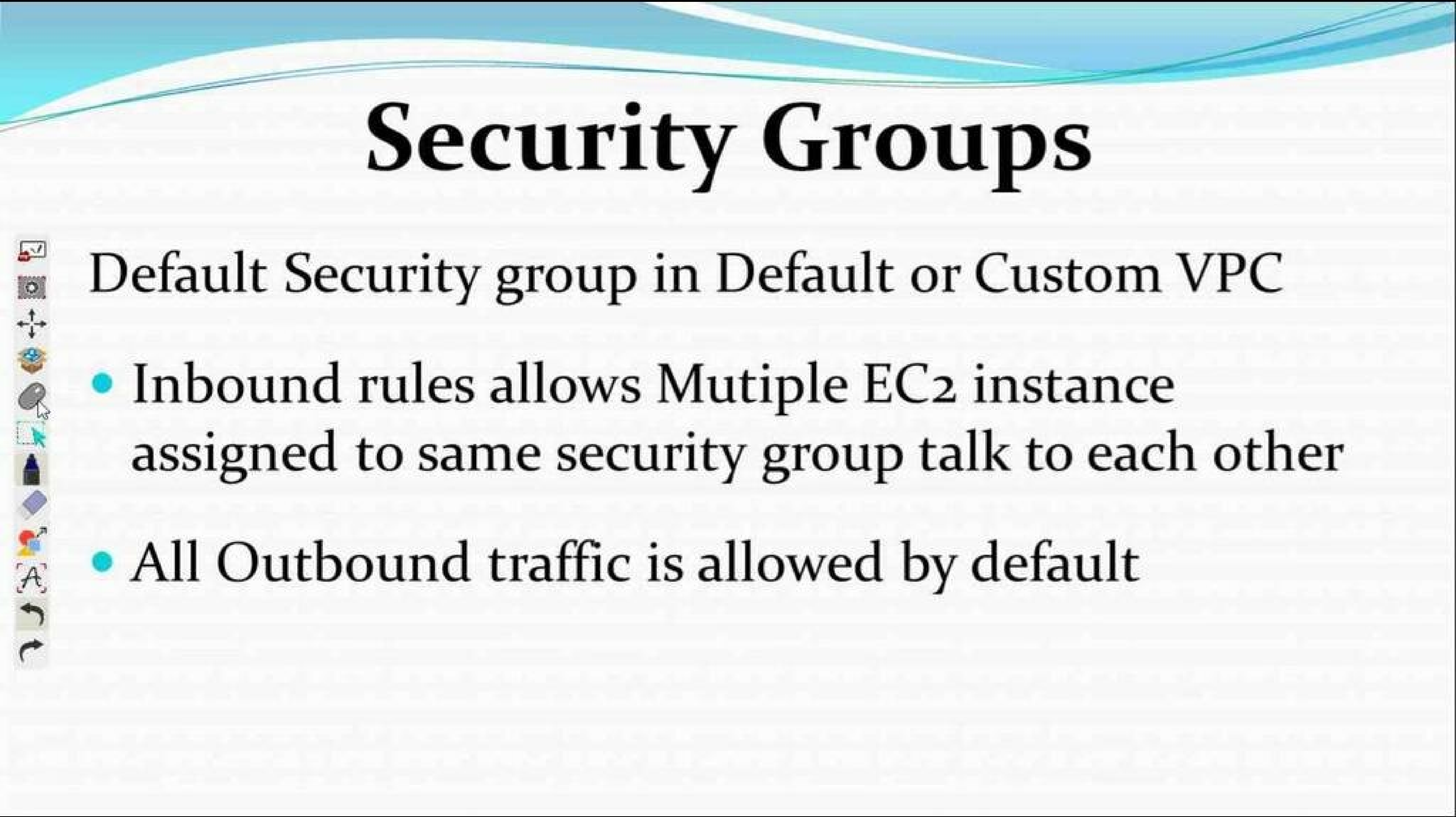
- Inbound rules allows Mutiple EC2 instance assigned to same security group talk to each other
- All Outbound traffic is allowed by default

A1 11 SG

Security Groups

Default Security group in Default or Custom VPC

- Inbound rules allows Mutiple EC2 instance assigned to same security group talk to each other
- All Outbound traffic is allowed by default



Security Groups

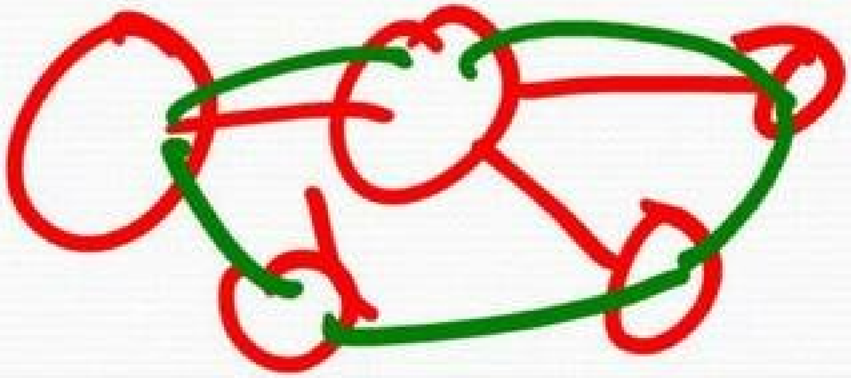
Default Security group in Default or Custom VPC

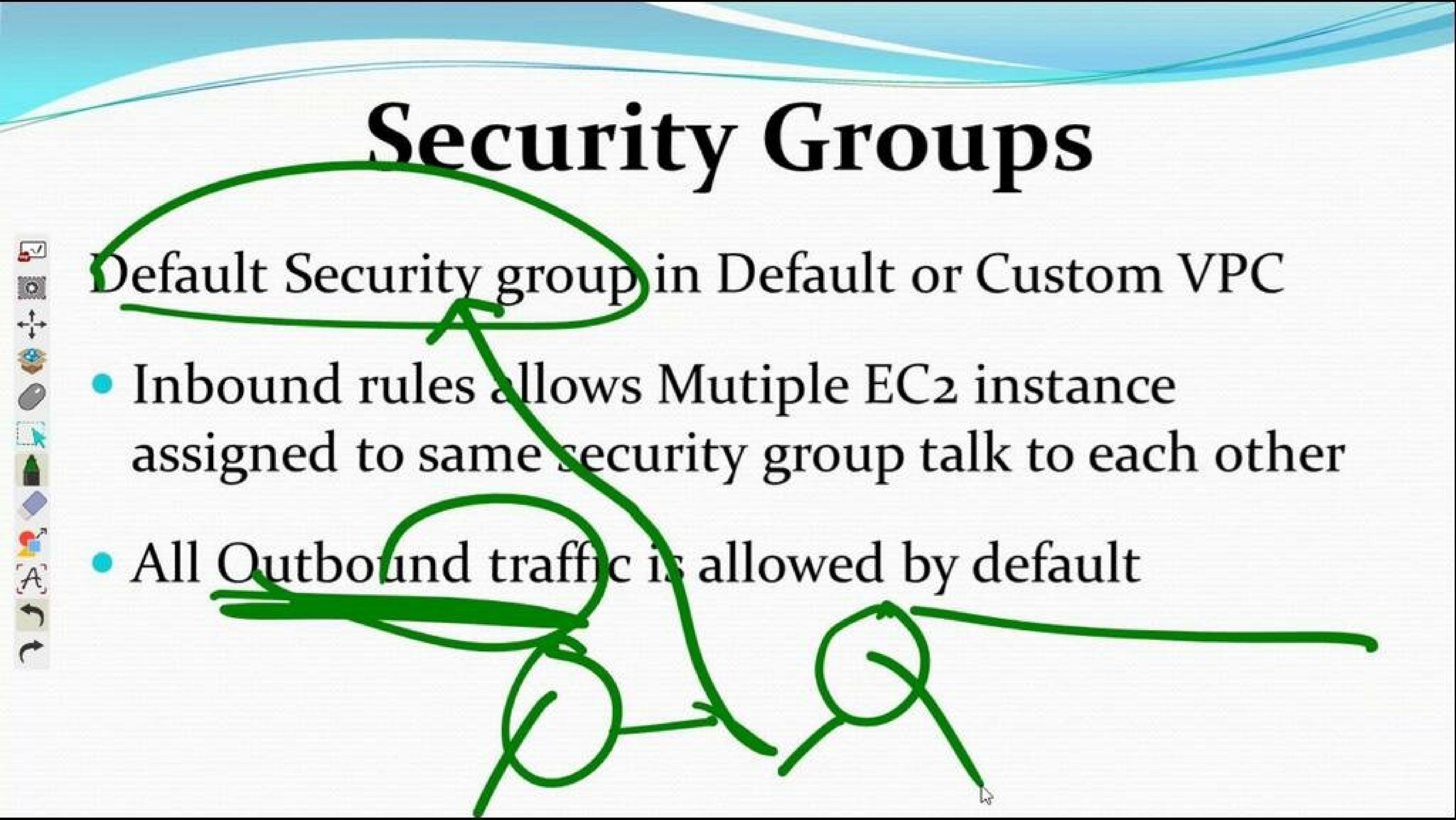
- Inbound rules allows Mutiple EC2 instance assigned to same security group talk to each other
- All Outbound traffic is allowed by default

Security Groups

Default Security group in Default or Custom VPC

- Inbound rules allows Mutiple EC2 instance assigned to same security group talk to each other
- All Outbound traffic is allowed by default





Security Groups

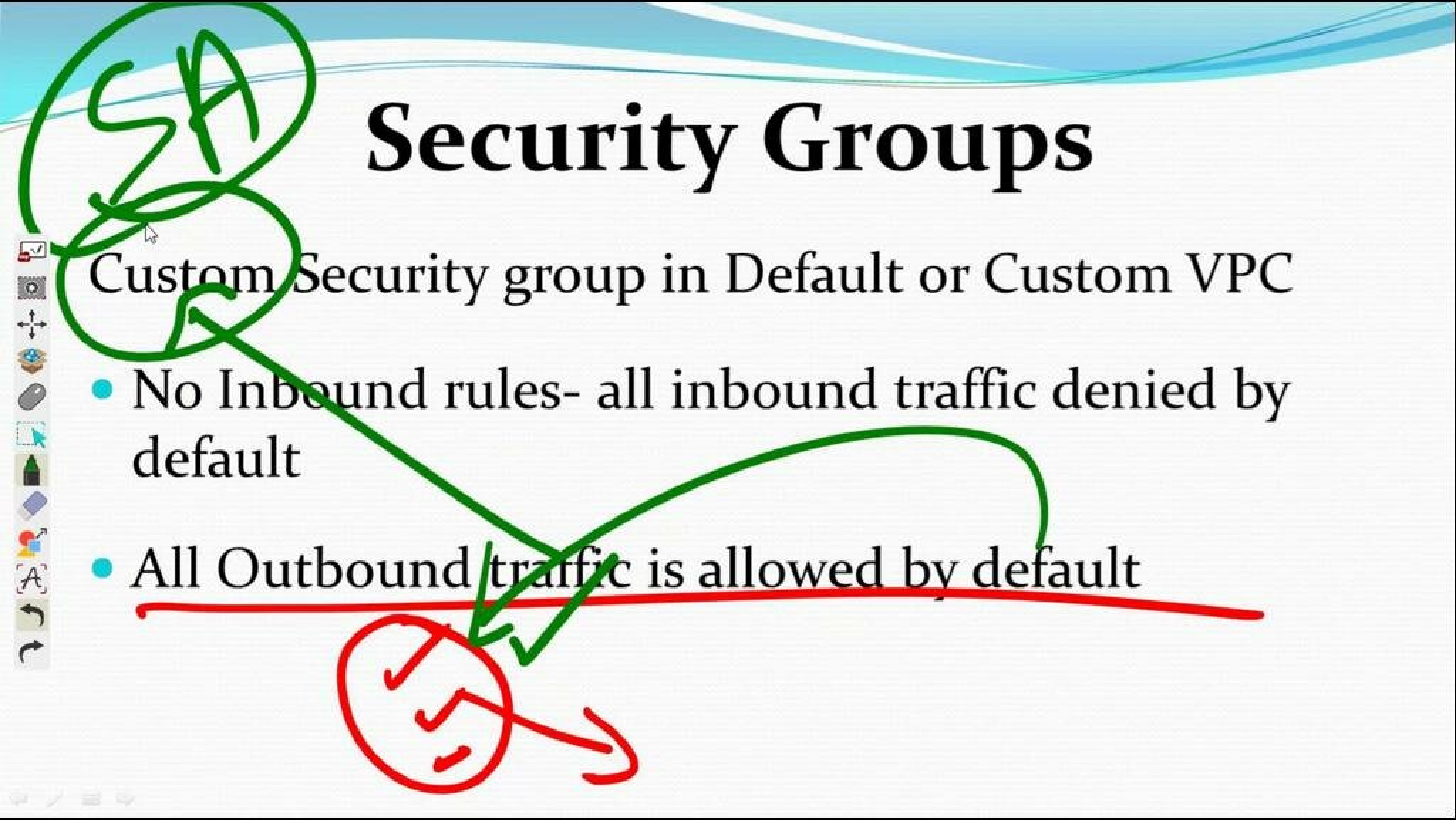
Default Security group in Default or Custom VPC

- Inbound rules allows Mutiple EC2 instance assigned to same security group talk to each other
- All Outbound traffic is allowed by default

Security Groups

Custom Security group in Default or Custom VPC

- No Inbound rules- all inbound traffic denied by default
- All Outbound traffic is allowed by default



SA

Security Groups

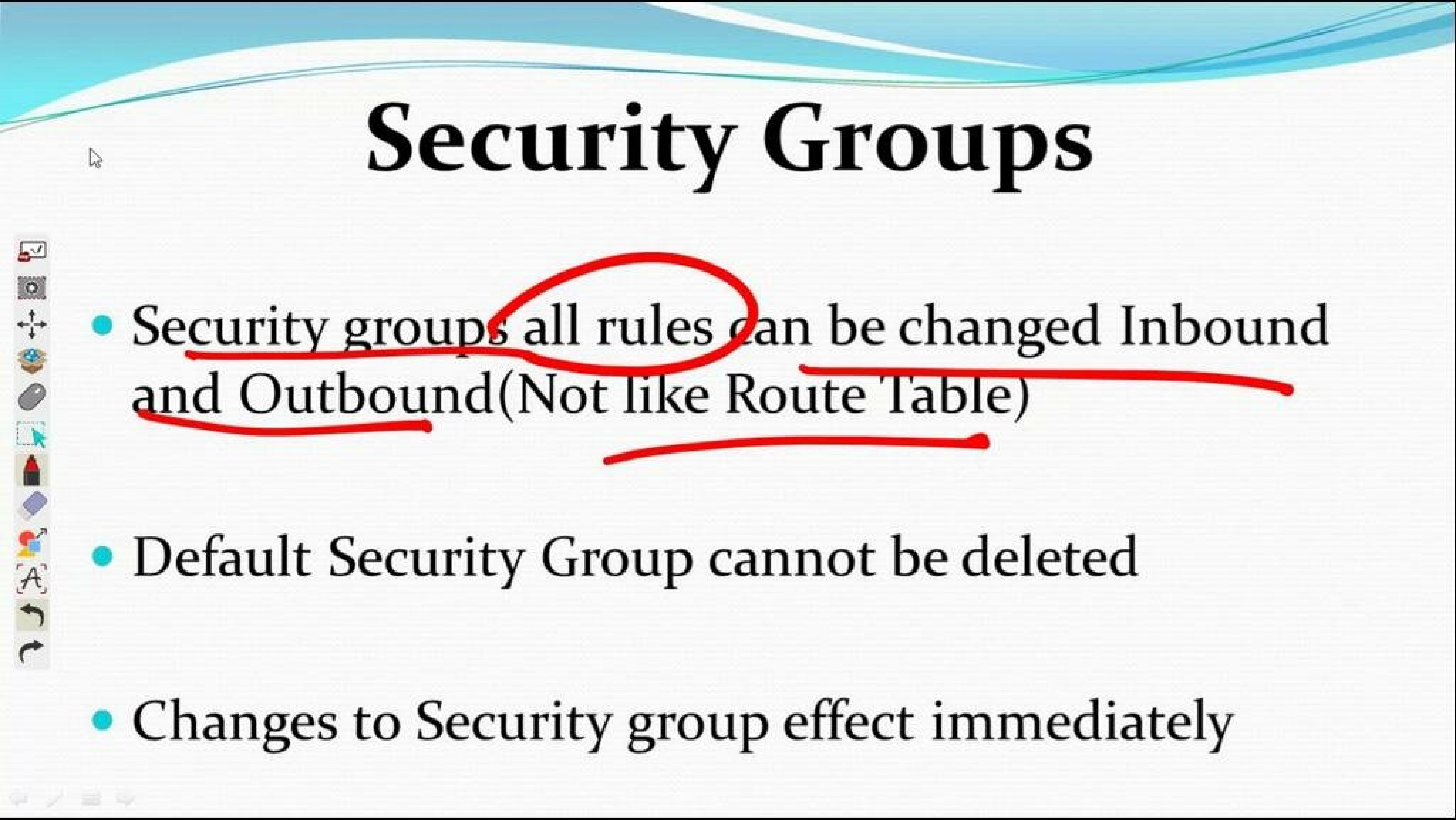
Custom Security group in Default or Custom VPC

- No Inbound rules- all inbound traffic denied by default
- All Outbound traffic is allowed by default

Security Groups

Custom Security group in Default or Custom VPC

- No Inbound rules- all inbound traffic denied by default
- All Outbound traffic is allowed by default

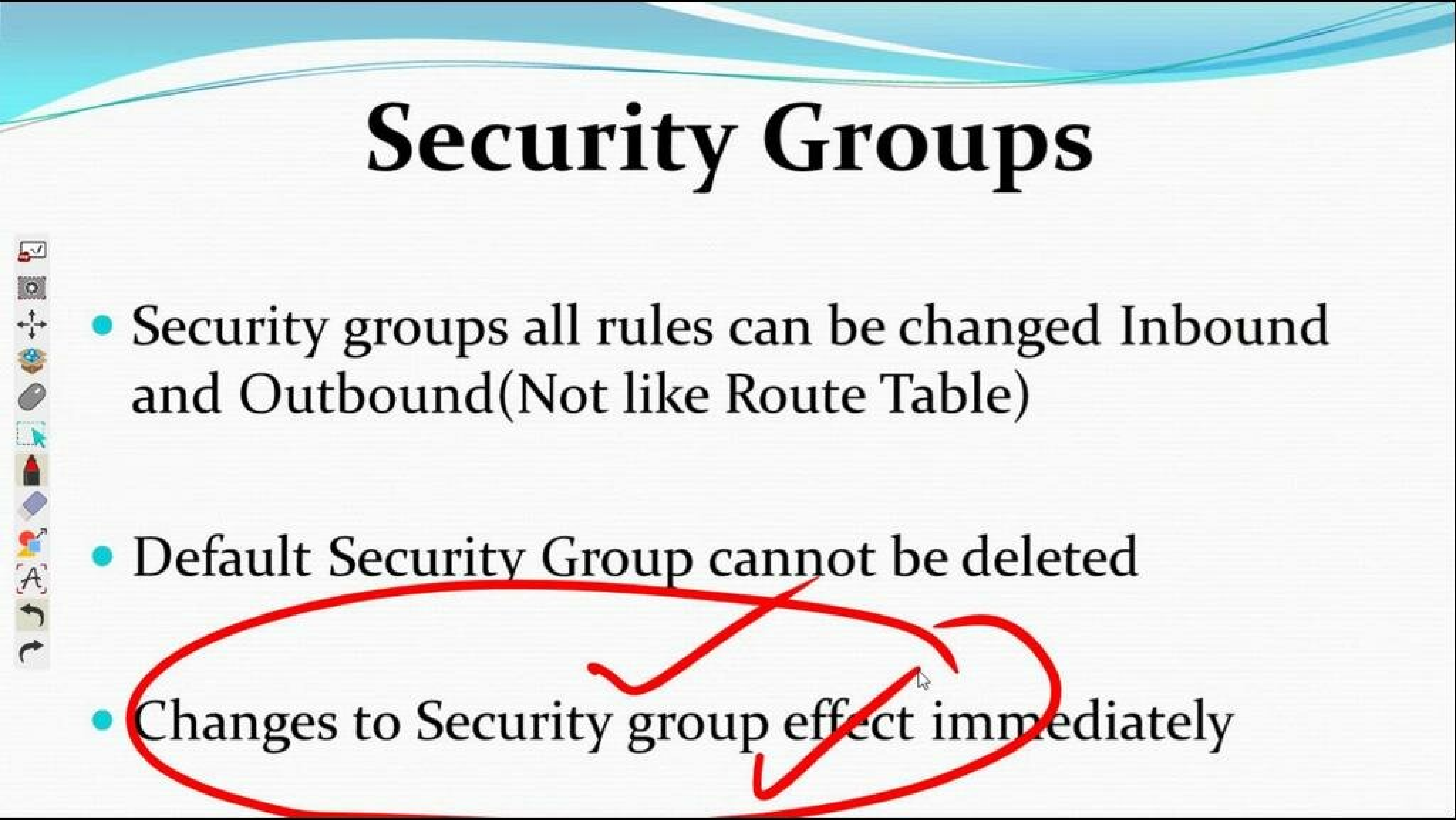


Security Groups

- Security groups all rules can be changed Inbound and Outbound(Not like Route Table)
- Default Security Group cannot be deleted
- Changes to Security group effect immediately

Security Groups

- Security groups all rules can be changed Inbound and Outbound(Not like Route Table)
- Default Security Group cannot be deleted
- Changes to Security group effect immediately

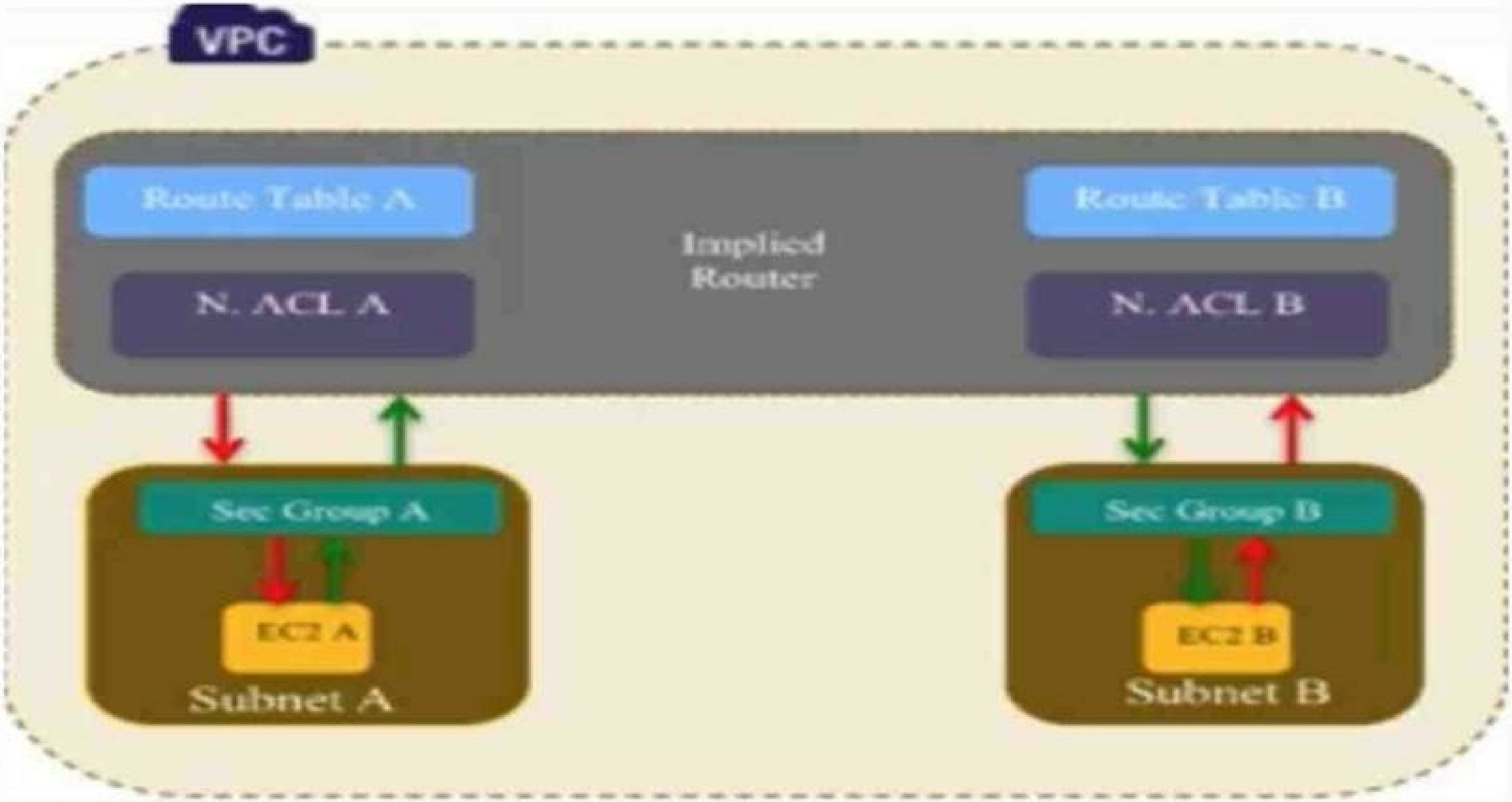


Security Groups

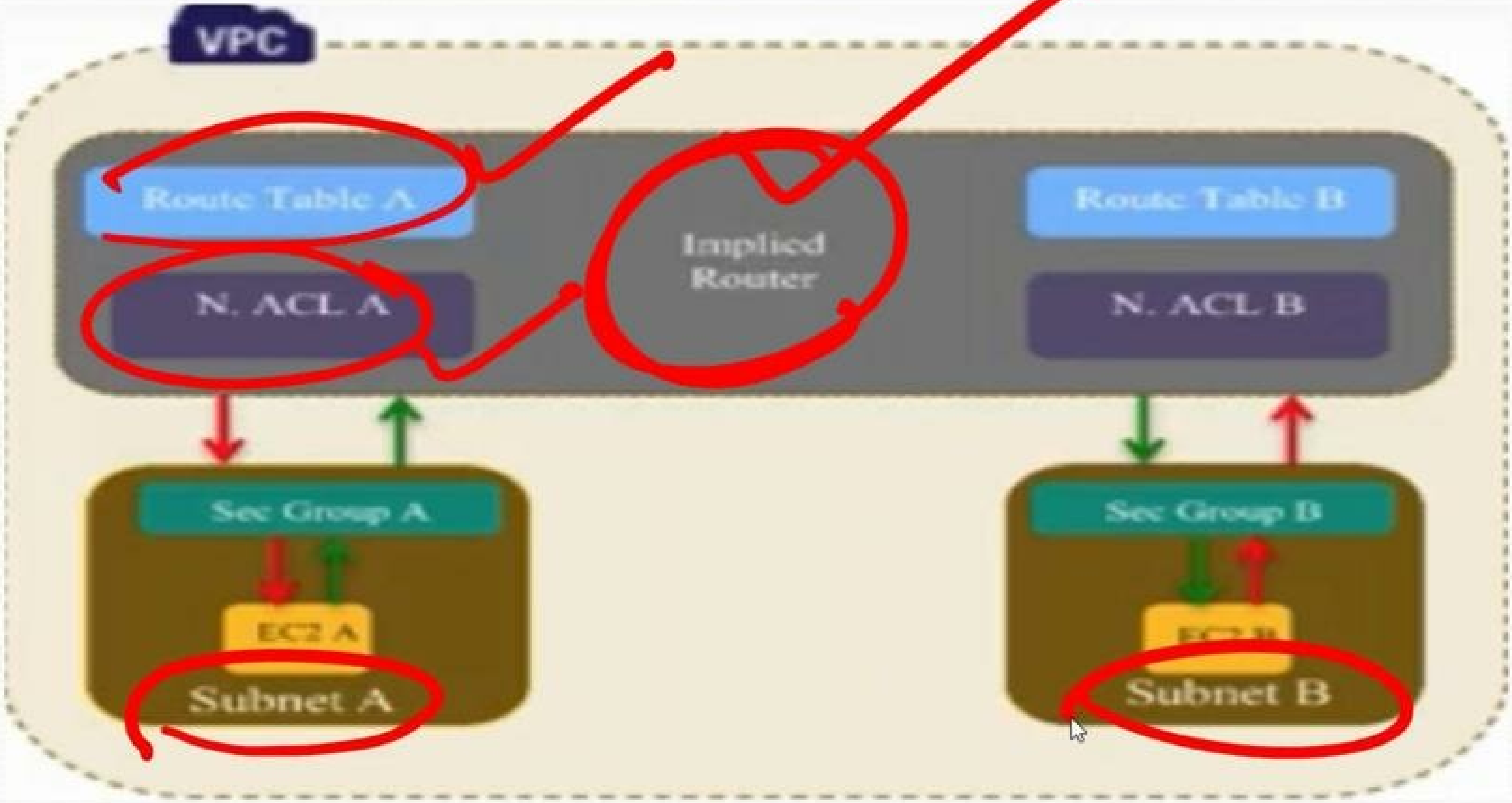
- Security groups all rules can be changed Inbound and Outbound(Not like Route Table)
- Default Security Group cannot be deleted
- Changes to Security group effect immediately

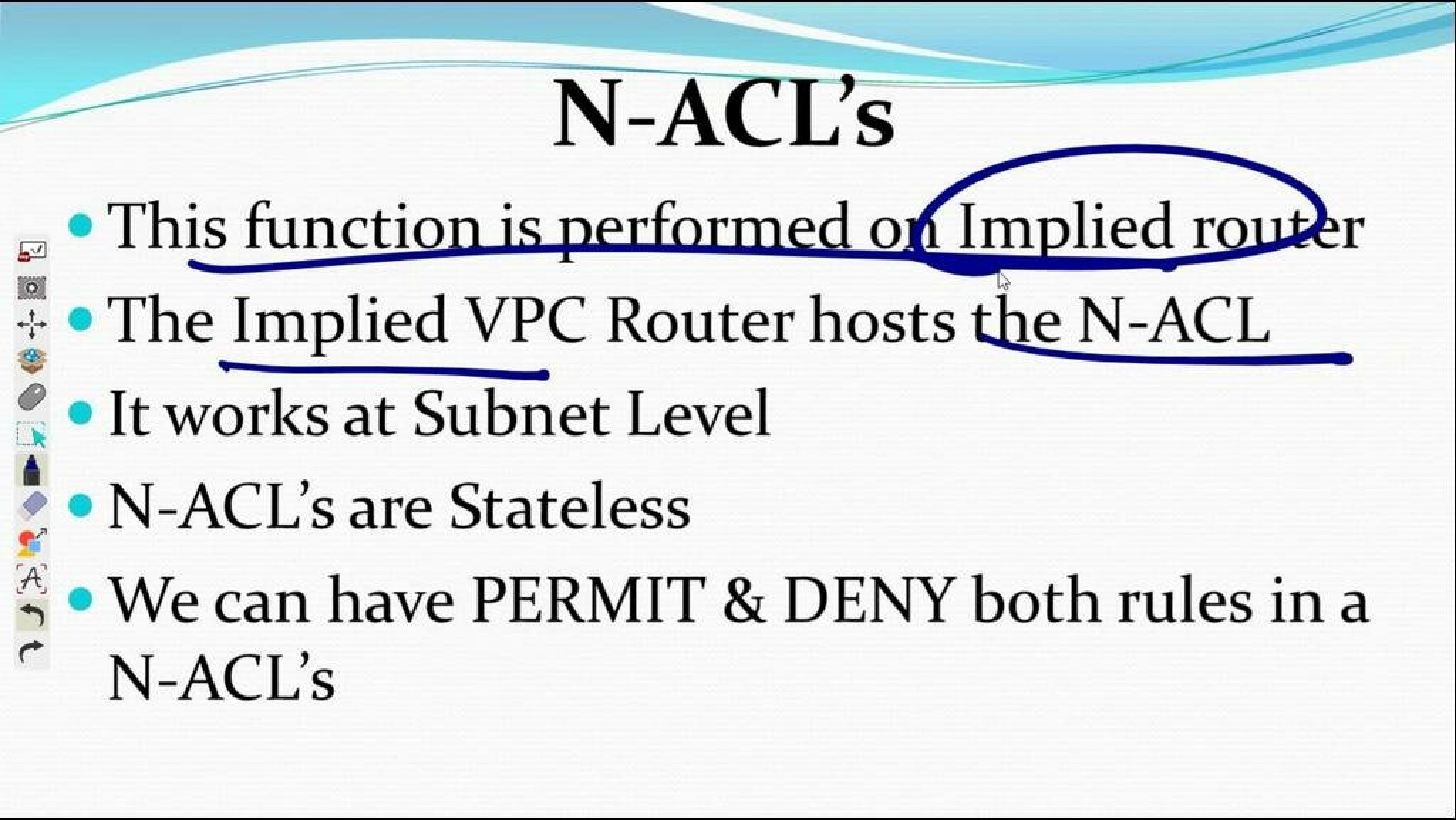
Network Access Control List

N-ACL’s


VPC
Route Table A
Implied Router
Route Table B
N. ACL A
N. ACL B
Sec Group A
Sec Group B
EC2 A
EC2 B
Subnet A
Subnet B

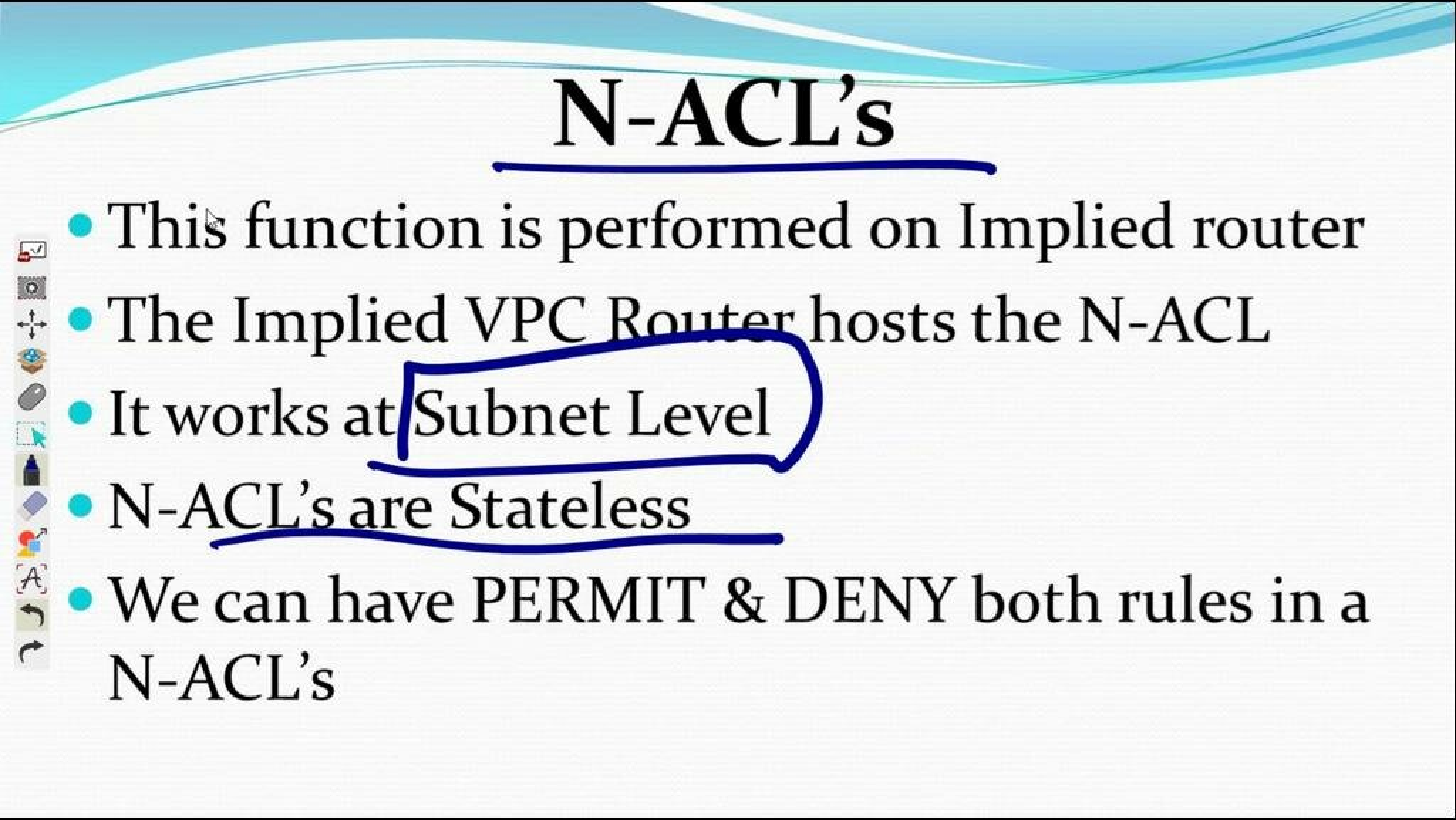
N-ACL's


VPC
Route Table A
N. ACL A
Implied Router
Route Table B
N. ACL B
Sec Group A
EC2 A
Subnet A
Sec Group B
EC2 B
Subnet B



N-ACL’s

- This function is performed on Implied router
- The Implied VPC Router hosts the N-ACL
- It works at Subnet Level
- N-ACL’s are Stateless
- We can have PERMIT & DENY both rules in a N-ACL’s

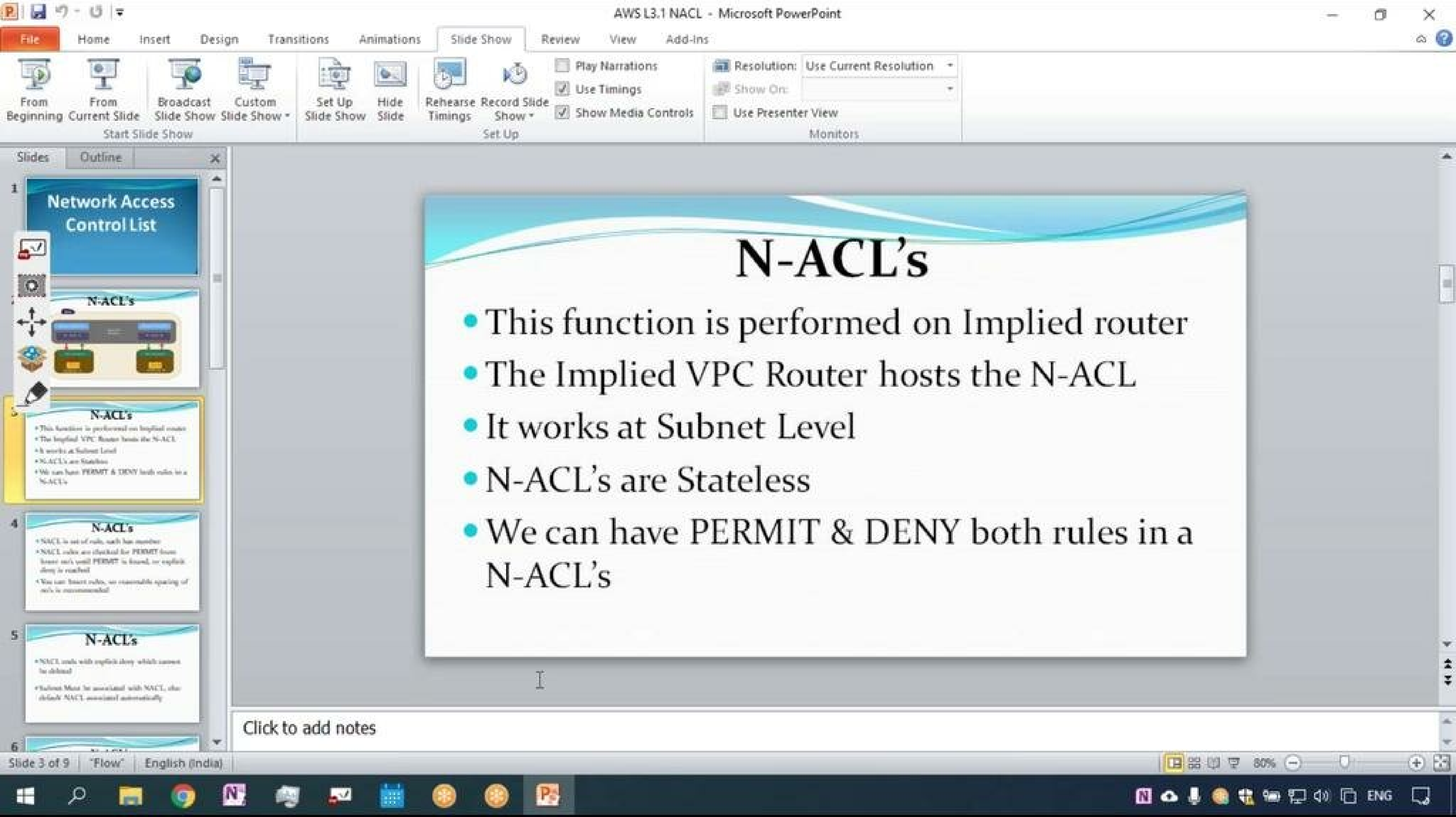


N-ACL’s

- This function is performed on Implied router
- The Implied VPC Router hosts the N-ACL
- It works at Subnet Level
- N-ACL’s are Stateless
- We can have PERMIT & DENY both rules in a N-ACL’s

N-ACL's

- This function is performed on Implied router
- The Implied VPC Router hosts the N-ACL
- It works at Subnet Level
- N-ACL's are Stateless
- We can have PERMIT & DENY both rules in a N-ACL's

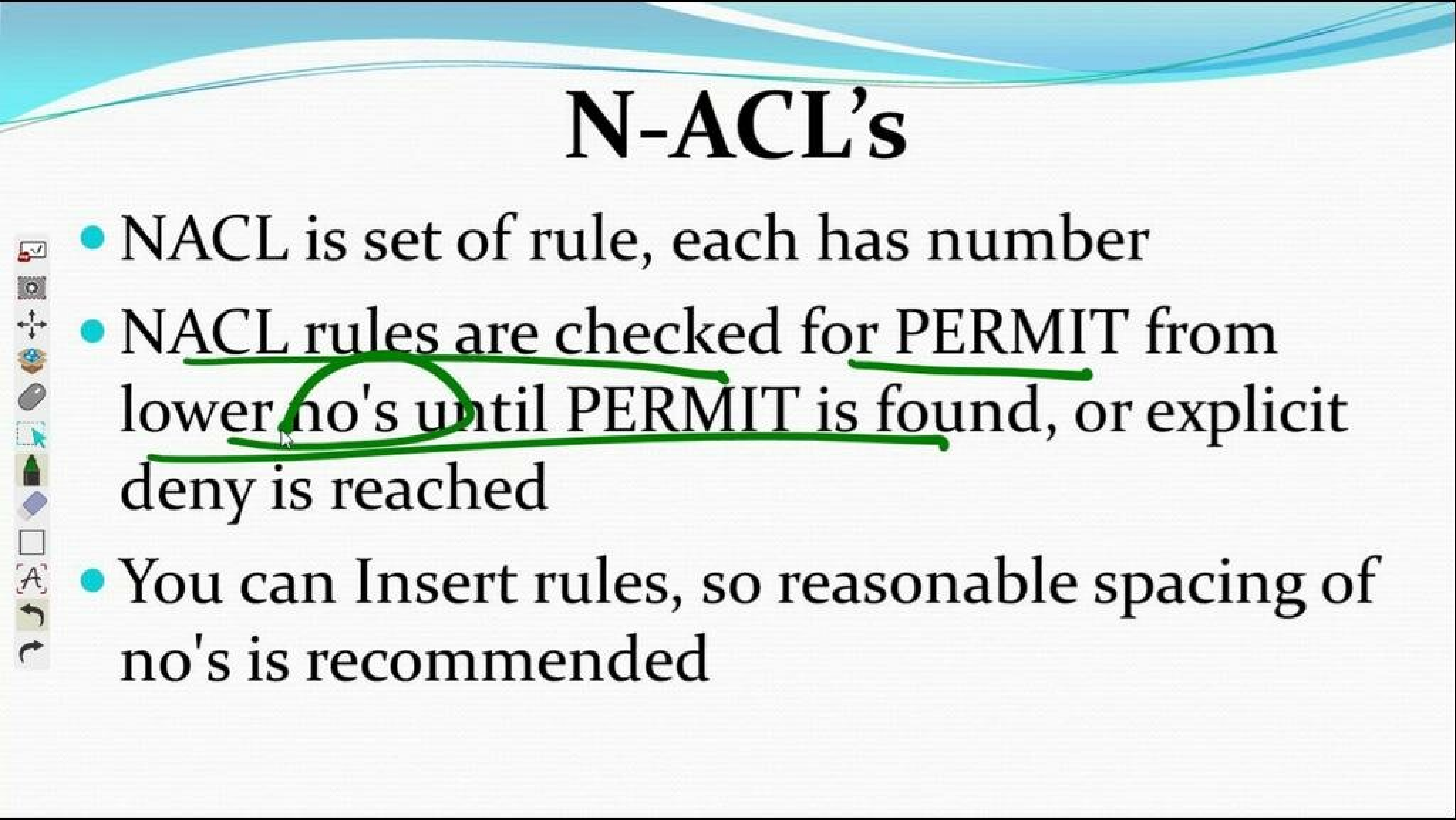


□ Play Narrations
☑ Use Timings
☑ Show Media Controls

Resolution: Use Current Resolution
Show On:
□ Use Presenter View

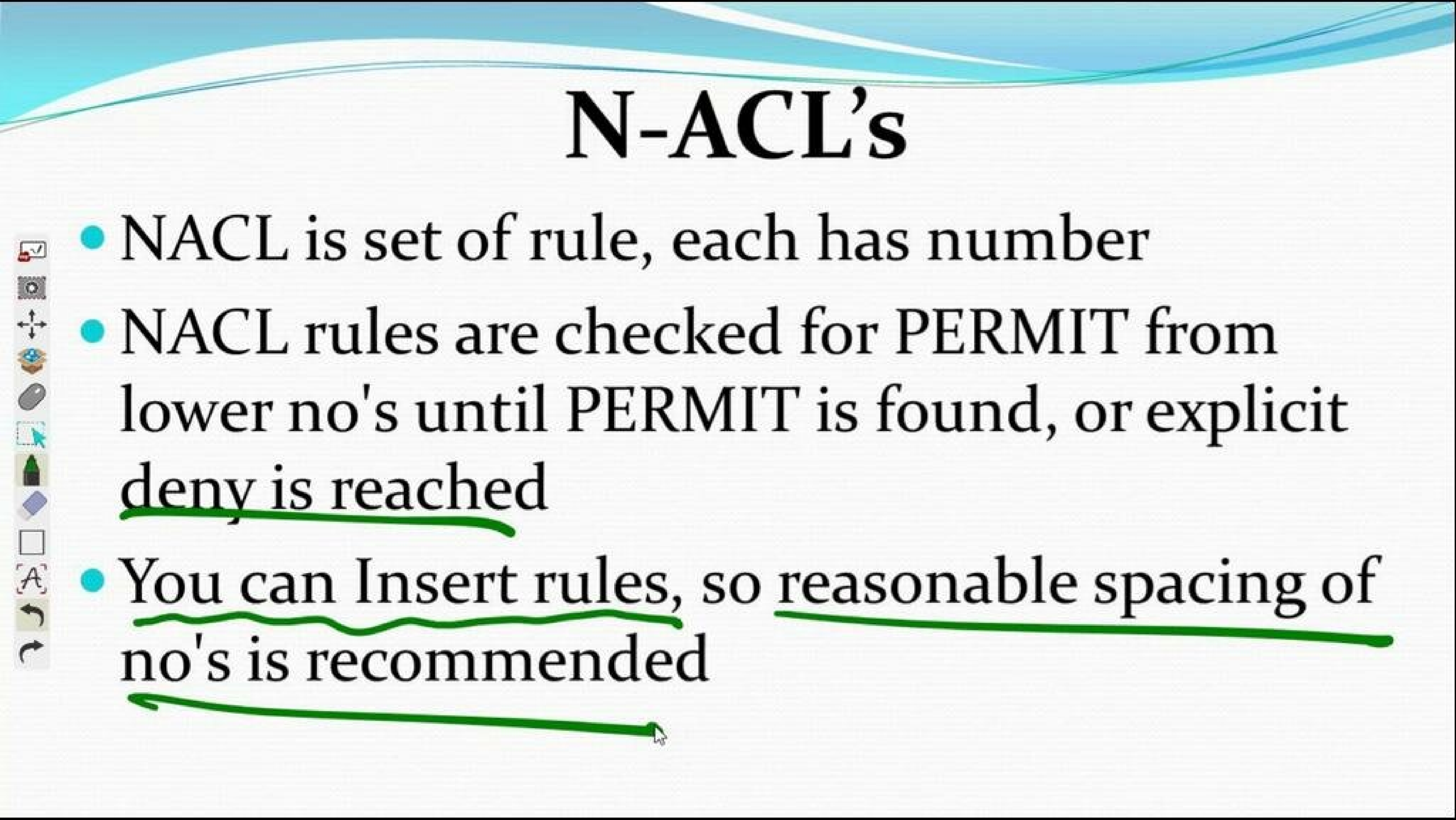
N-ACL's

- This function is performed on Implied router
- The Implied VPC Router hosts the N-ACL
- It works at Subnet Level
- N-ACL's are Stateless
- We can have PERMIT & DENY both rules in a N-ACL's



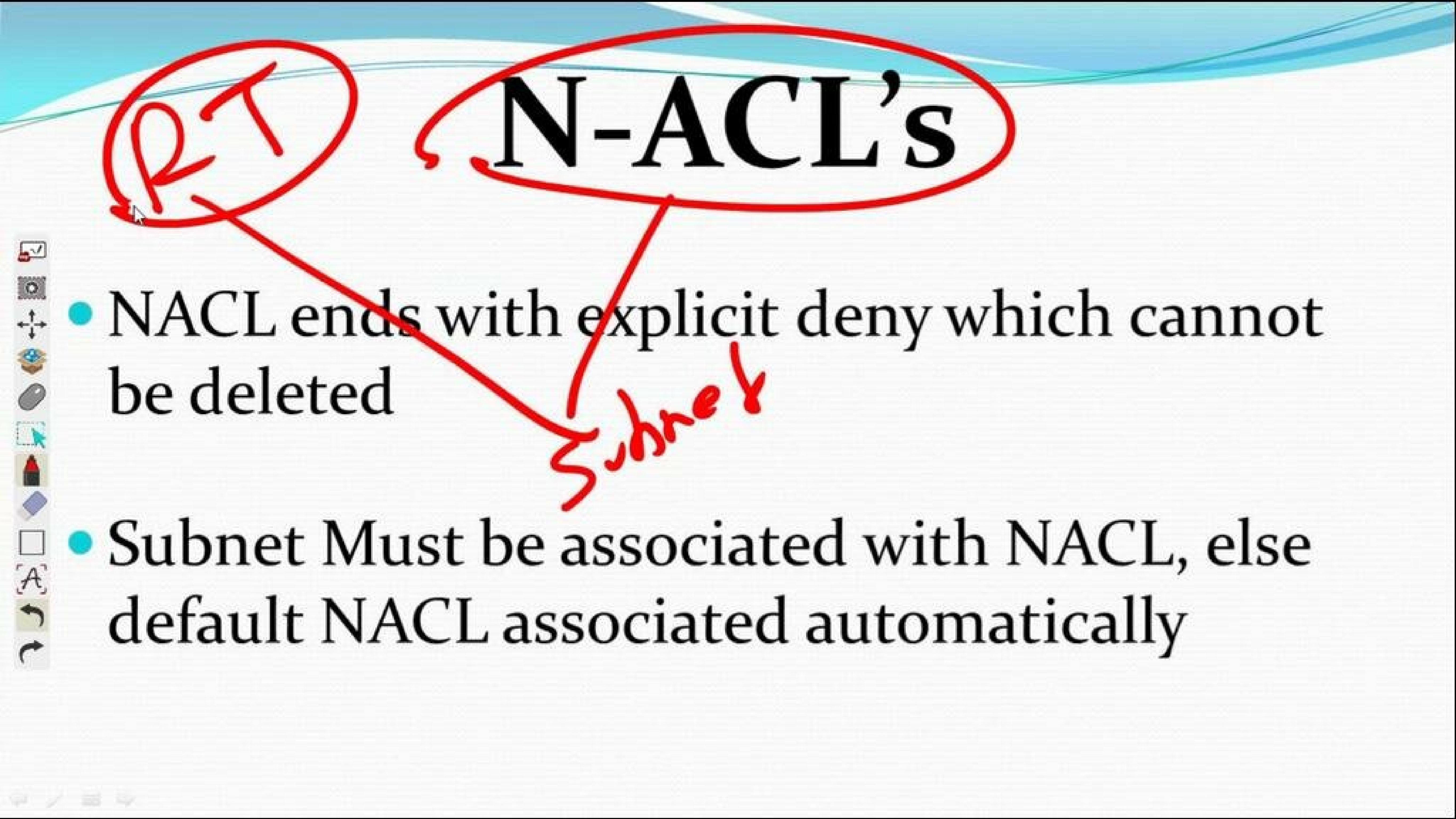
N-ACL's

- NACL is set of rule, each has number
- NACL rules are checked for PERMIT from lower no's until PERMIT is found, or explicit deny is reached
- You can Insert rules, so reasonable spacing of no's is recommended



N-ACL's

- NACL is set of rule, each has number
- NACL rules are checked for PERMIT from lower no's until PERMIT is found, or explicit deny is reached
- You can Insert rules, so reasonable spacing of no's is recommended



N-ACL's

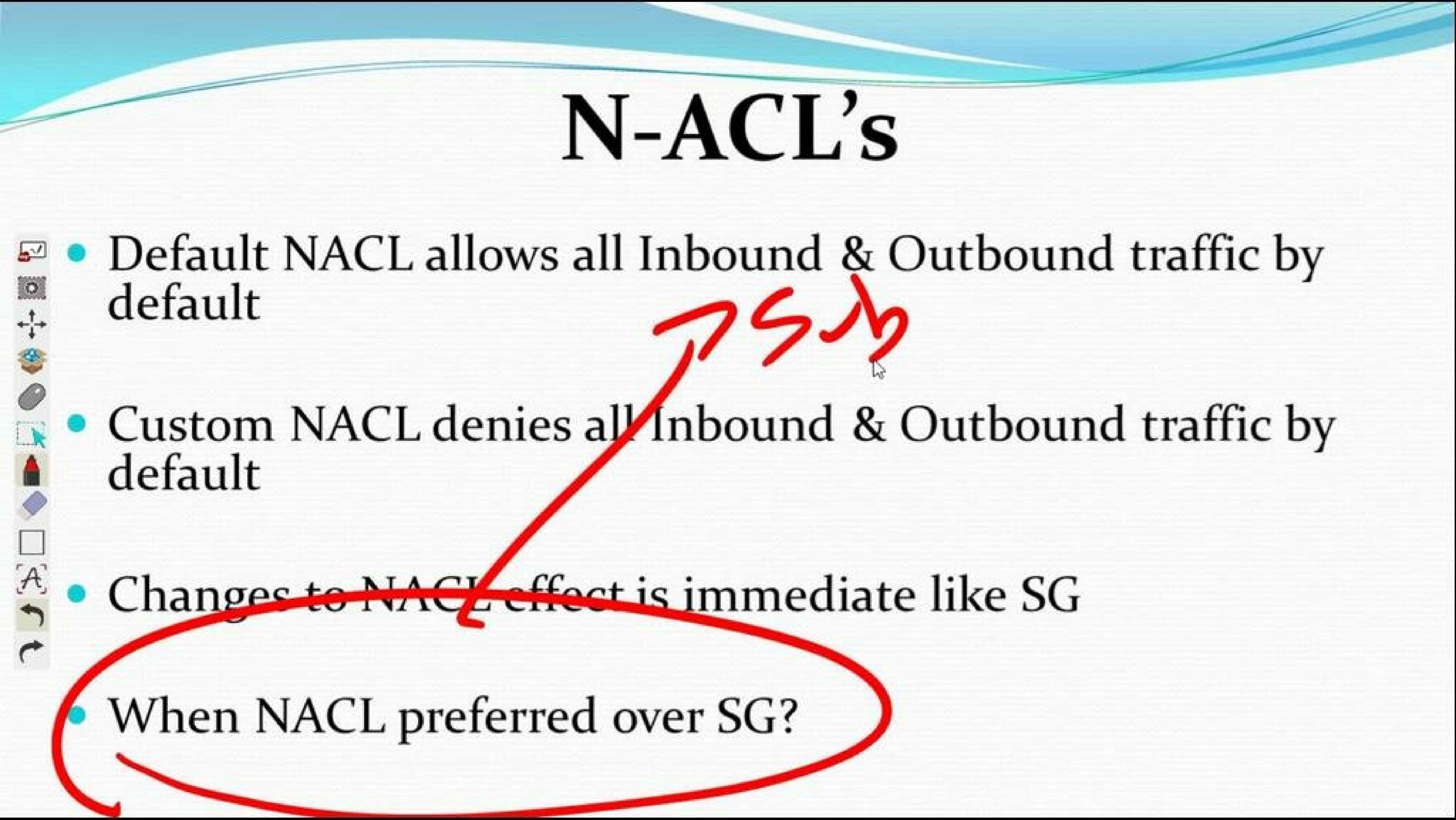
- NACL ends with explicit deny which cannot be deleted
- Subnet Must be associated with NACL, else default NACL associated automatically

N-ACL’s

- Default NACL allows all Inbound & Outbound traffic by default
- Custom NACL denies all Inbound & Outbound traffic by default
- Changes to NACL effect is immediate like SG
- When NACL preferred over SG?

N-ACL's

- Default NACL allows all Inbound & Outbound traffic by default
- Custom NACL denies all Inbound & Outbound traffic by default
- Changes to NACL effect is immediate like SG
- When NACL preferred over SG?



N-ACL’s

- Default NACL allows all Inbound & Outbound traffic by default

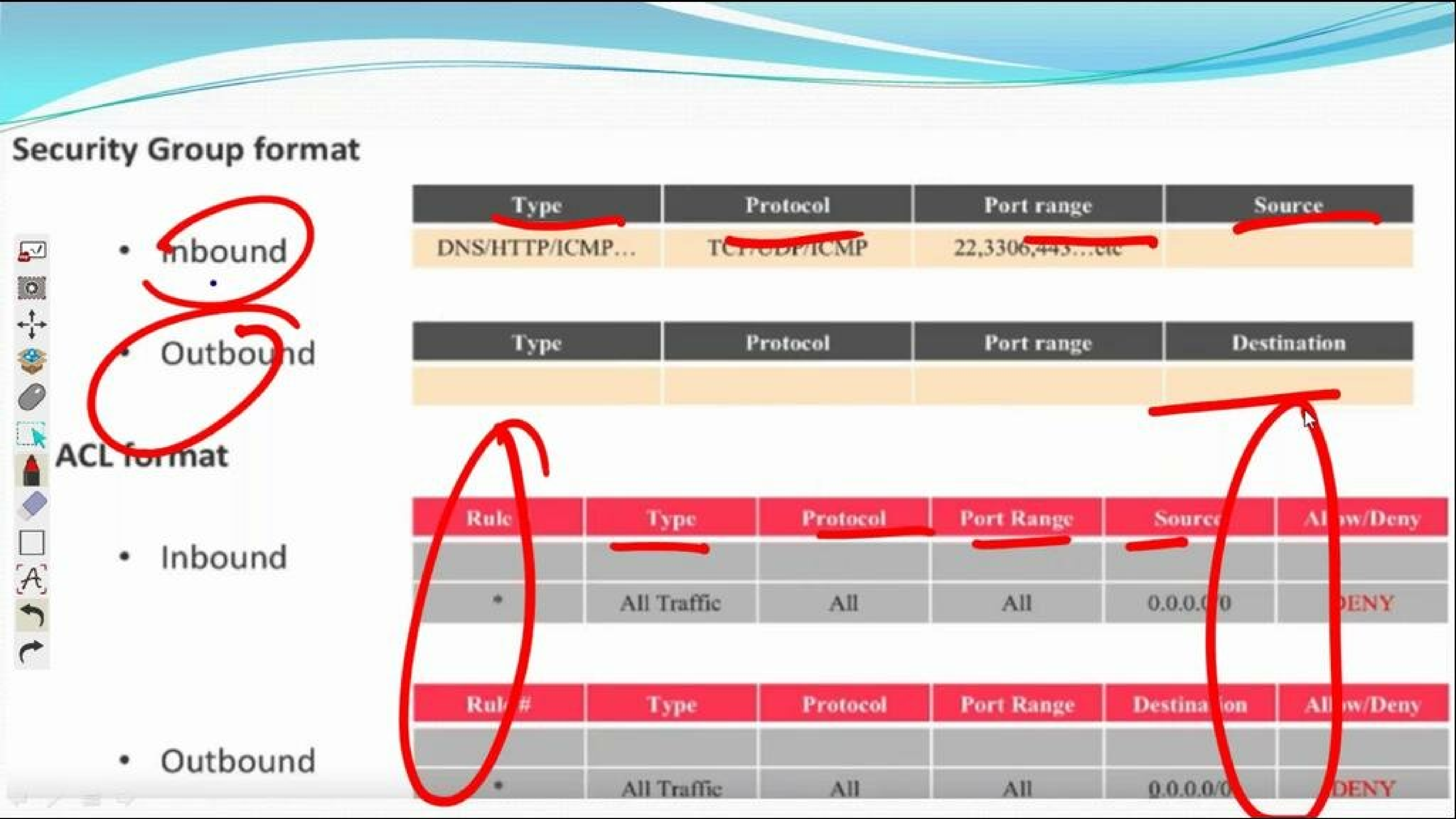
SG

- Custom NACL denies all Inbound & Outbound traffic by default
- Changes to NACL effect is immediate like SG
- When NACL preferred over SG?

N-ACL’s

- Inbound in NACL means coming from outside subnet. Outbound means going out of Subnet

- Inbound for SG means coming from outside the instance. Outbound means going out of Instance ENI



Security Group format

- Inbound

Type	Protocol	Port range	Source
DNS/HTTP/ICMP…	TCP/UDP/ICMP	22,3306,443…etc	

- Outbound

Type	Protocol	Port range	Destination

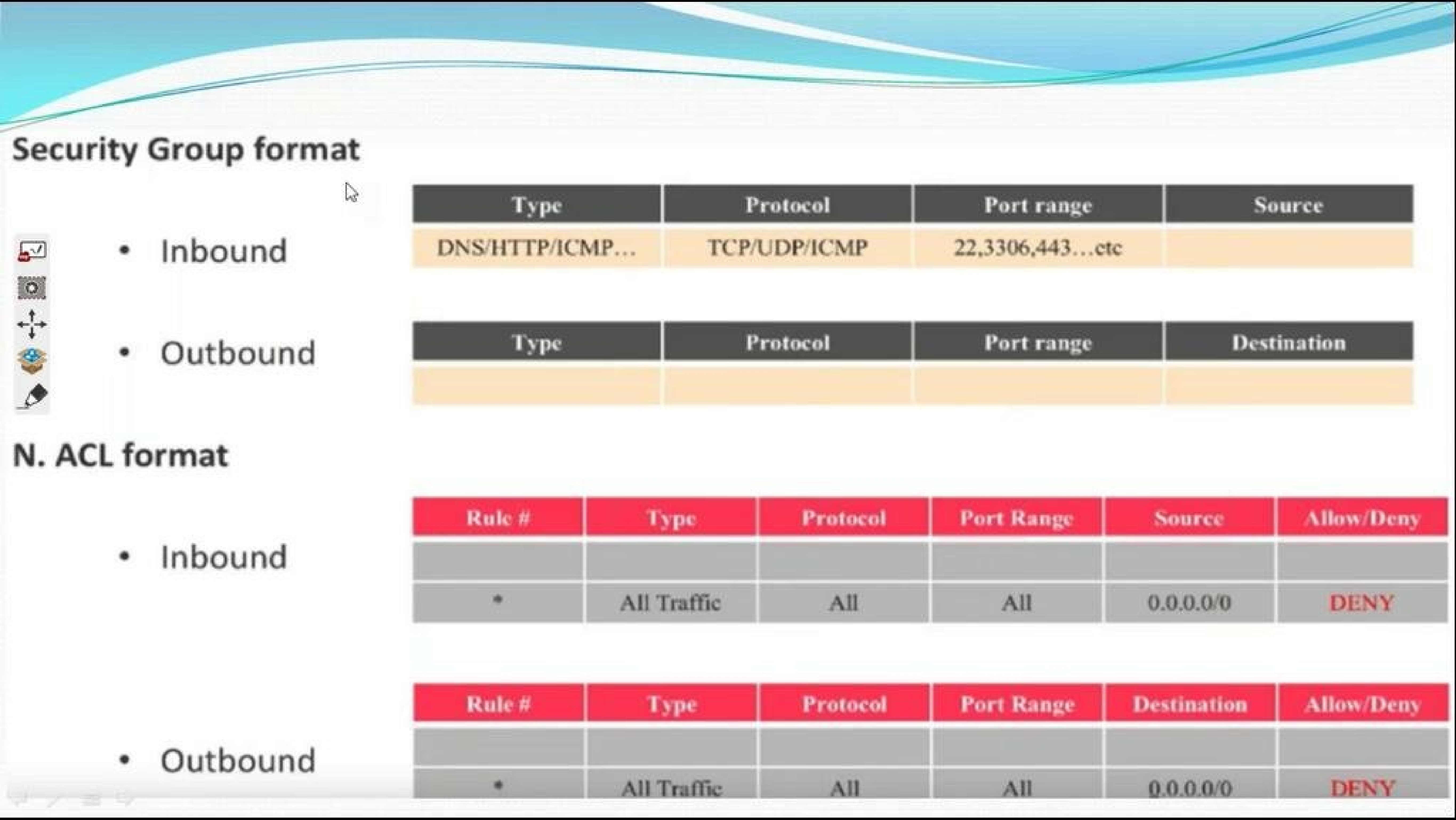
ACL format

- Inbound

Rule	Type	Protocol	Port Range	Source	Allow/Deny
*	All Traffic	All	All	0.0.0.0/0	DENY

- Outbound

Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
*	All Traffic	All	All	0.0.0.0/0	DENY



Security Group format

- Inbound

Type	Protocol	Port range	Source
DNS/HTTP/ICMP…	TCP/UDP/ICMP	22,3306,443…etc	

- Outbound

Type	Protocol	Port range	Destination

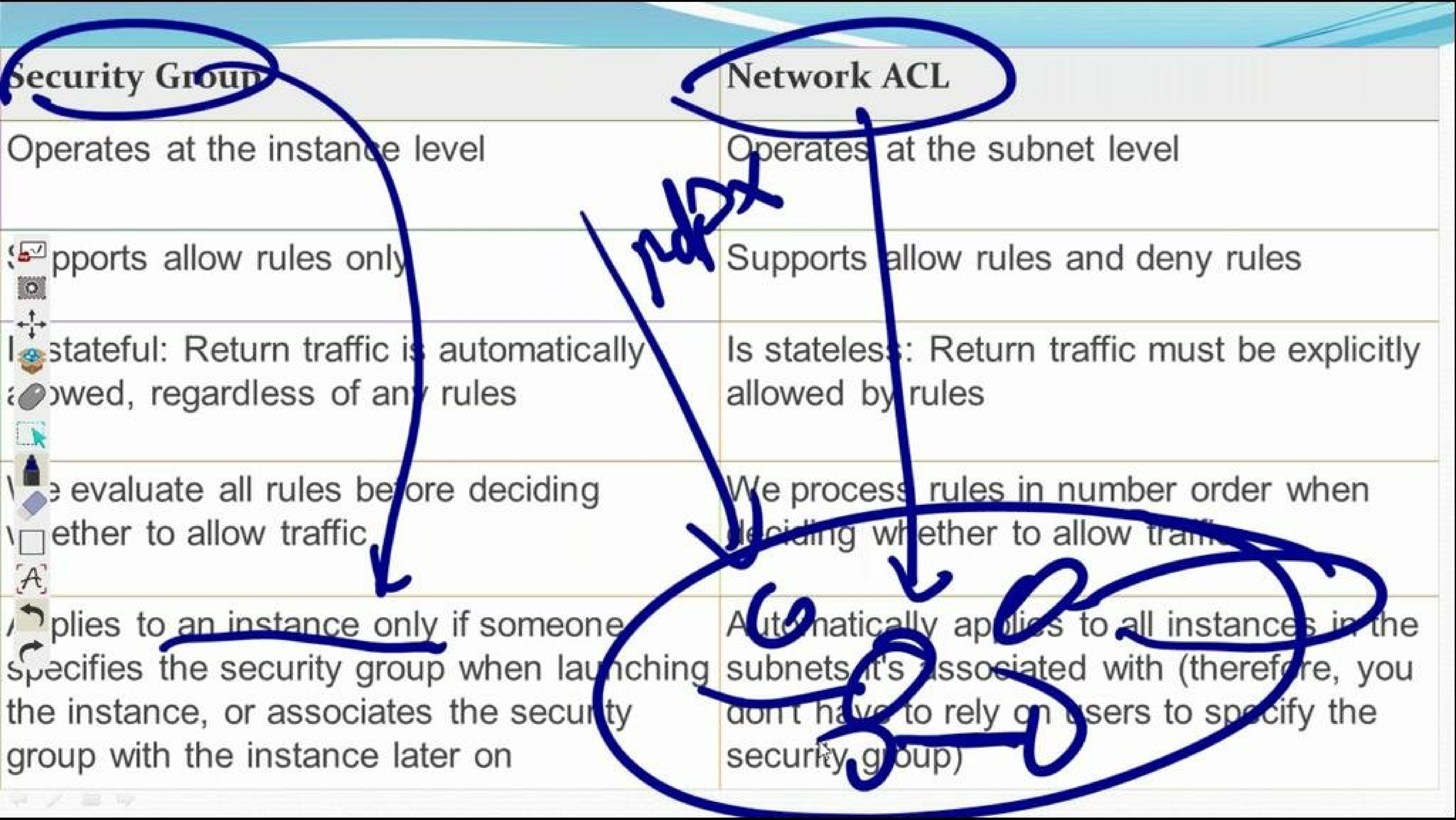
N. ACL format

- Inbound

Rule #	Type	Protocol	Port Range	Source	Allow/Deny
*	All Traffic	All	All	0.0.0.0/0	DENY

- Outbound

Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
*	All Traffic	All	All	0.0.0.0/0	DENY
)



Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (therefore, you don't have to rely on users to specify the security group)