

NETSEC-001 - Define security best practices for Virtual Private Cloud (Amazon VPC) and other network security considerations

Based on the methodology and design of the solution, security groups are defined in such a way as to allow traffic only to and from where it belongs.

Considerations:

The entire implemented environment required a Landing Zone. Here we defined the VPC to be used and the security groups that would allow us to define access and restrictions for incoming and outgoing traffic.

At the security group level

- AppStream instances internet traffic goes through a nat instance
- All EC2s are in private subnets.

Instances (1) [Info](#)

Find Instance by attribute or tag (case-sensitive)						All states ▼
<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check	
<input type="checkbox"/>	NAT	i-011d545ffbc399535	Running	t4g.nano	3/3 checks passed	

Route tables (1/3) [Info](#)

Find resources by attribute or tag					
<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main
<input checked="" type="checkbox"/>	autohallVPC-MainRoute	rtb-078cc37f06da9302c	-	-	Yes
<input type="checkbox"/>	-	rtb-01232c1d0b28d7cf2	-	-	Yes
<input type="checkbox"/>	autohallVPC-PublicRoute	rtb-03ee86590505241a1	6 subnets	-	No

rtb-078cc37f06da9302c / autohallVPC-MainRoute

Details [Routes](#) Subnet associations Edge associations Route propagation Tags

Routes (3)

Filter routes		
Destination	Target	Status
pl-63a5400a	vpce-0f66c4d0e92347080	Active
0.0.0.0/0	eni-0706d8e4047e8c017	Active
10.0.0.0/20	local	Active