vpc lan nate gate awy and peering

vpc lab

start vpc wizard

your vpcs ---

create vpc ----name
cidr block
ipv6 cidr
tenancy
create
vpc id cidr route table networkacl summery cidrblock

action----delete edit dhcpoptions dnsresolutions dnshostname createflowlog

subnet
create subnet
name ----------publicsubnet
vpc---select
availibilty zone
cidr block
create subnet
name -------privatesubnet
vpc
availibiltyzone
cidr block

action ----delete , edit cidr , ecit network acl association , edit route table association
cidr reservation

Routing Table
default routing table

route----default
so route table
public
private

create a new route table ----public
creat a new routing table --------private

Intenet Gateway

create a internetgateway-----name

Attach VPC------most imp

action ----attach deattach

public routing table
edit route
0.0.0.0/0 IGW

in routing table--------subnet association
public edit---publicsubnet

in private routing table---subnet associte
edit--privatesubnet

EC2 instance----launch --instance--server--configure--network --vpc(own)--
subnet(private)--auto assign ip address---add storage and tag ---launch

2 nd instance ---launch---private ----auto assign ip address---launch

do no ko public ip
private ko----no internet gateway

access public
not access private subnet

public subnet----private subnet (EC2)---private ip

public ec2----remote desktop---private ka private ip

vpc lan nate gate awy and peering

NAT Gateway

enable instance in private subnet to connect intenet or another aws service

prevent internet from initializing connection with thos instance

package download and update

chargable ---nat gateway and data processinfg rate

nat gateway must specify the public subnet

must also specify an elastic ip address

no need to assign public ip to private instance

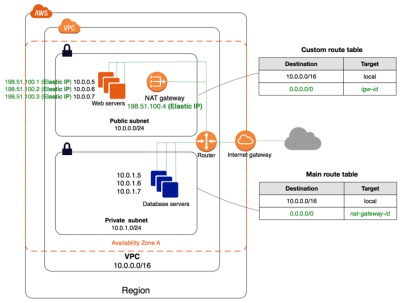
after create a nat gateway you must upgrade route table

private subnet to point internet traffic to the nat gateway

you have limit of number of gateway

natgateway-elastic ip address

deleting gateway diassociate elastic ip



1----create vpc
name cidr create
2---subnet create--**public** name and vpc associate , availaibilty zone ,
ipv4 cidr block
note: defaullt vpc ---all subnet already create----all public
(convert public to private ?
every subnet have internet gateway
custom subnet setting by us --dont have egw by default)
3 create subnet
name --**private**, vpc , availibilty zone , cidr

4 internet gateway
create , name , attach to vpc

5 routing table
main routing table---already created
ediit---add route--0.0.0.0 /0 igw--------save

subnet associate----which associate subnet ---goes on internet

---create a routing table---name private vpc create

note----routing table ---1 public 2 private ---easy identify

no edit------no internet
associte -----subnet private

subnet ----select ---action ----auto assign ip addess
✔ enable---check

private---subnet - aoto assign ip
uncheck enable

EC2 instance --1--- launch--server 2016----network myvpc ---subnet public
auto assign ip address ---enable---next----name

2 --launch--network myvpc --subnet private aoto assign ip disable
next --name ---
nat gateway---create ---subnet : public subnet , elastic ip ---create new ip---create

routing table----private----routes --- pahle check and than apply natgateway

vpc me elastic ip aa gaya hoga ---natgateway delete karoge to elastic ip delete nahi hoga

ec2 instance----public ---access --connected---login

public se ---private ec2 acess ---remote desktop---connect

private ec2 me no public ip address

ping 8.8.8.8 -t------no route

vpc--- route table---private route---edit--0.0.0.0/0 target netgateway---save

if internet gateway applt then public than anyone go on internet and access instance from internet

start ping----agar ham public ip assign kare to bhi access nahi kar sakte

ab ham natgateway delete ----trafic stop

elastic ip ----action deassociate

route table manually, subnet manually, internet gateway

delete vpc all are delete

ec2 instance delete ---terminate

vpc lan nate gate awy and peering

VPC PEERING
vpc peering enable connection between instance belongs to separate vpc

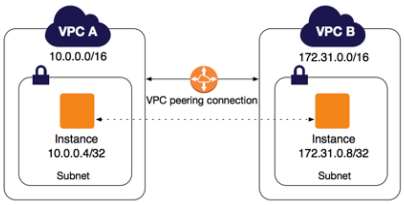
vpc peering use for connection between two vpc

use private address

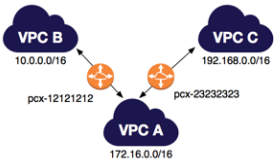
both belongs to different network range
if vpc single region or different region

inter region vpc peering

more than two aws account you can peer the vpc accross these accounts



multiple vpc peering connection



invalid vpc peering
overlaping CIDR
transitive peering
edge to edge routing through an internet gateway
edge to edge routing through private connection

overlaping CIDR

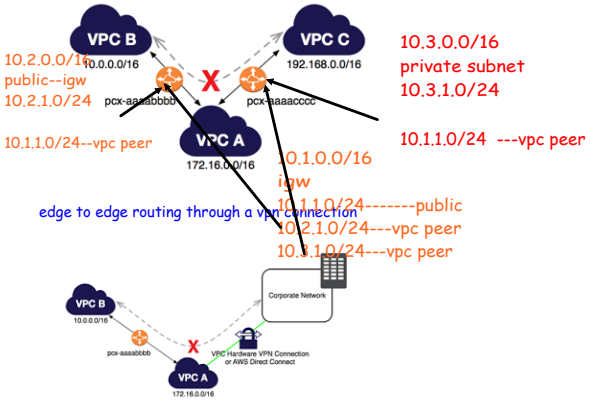
10.0.0.0/16
10.0.1.0/24

172.168.0.0/16
2001:12::1

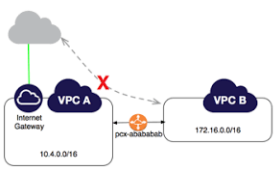
10.0.0.0/16
10.0.2.0/24

172.168.0.0/16
2001:13::1

transitive peering



edge to edge routing through private connection



vpc lan nate gate awy and peering

vpc peering configure

Route table	Destination	Target
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-11112222
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-11112222

vpc peering basic

vpc A vpc B both in only one account

one generate request another receive accept request

vpc A one account vpc B another account

routing table ---add cidr block and vpc peering id

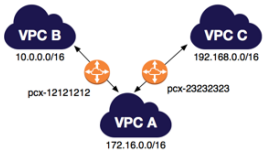
need to check security group

vpc peering create ---vpc peering id

two vpc with mutiple cidr peer together

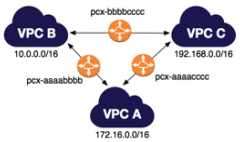
Route table	Destination	Target
VPC A	10.2.0.0/16	Local
	10.4.0.0/16	Local
	10.0.0.0/16	pcx-11112222
	10.3.0.0/16	pcx-11112222
VPC B	10.0.0.0/16	Local
	10.3.0.0/16	Local
	10.2.0.0/16	pcx-11112222
	10.4.0.0/16	pcx-11112222

one vpc peer with two vpcs



Route table	Destination	Target
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-12121212
	192.168.0.0/16	pcx-23232323
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-12121212
VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-23232323

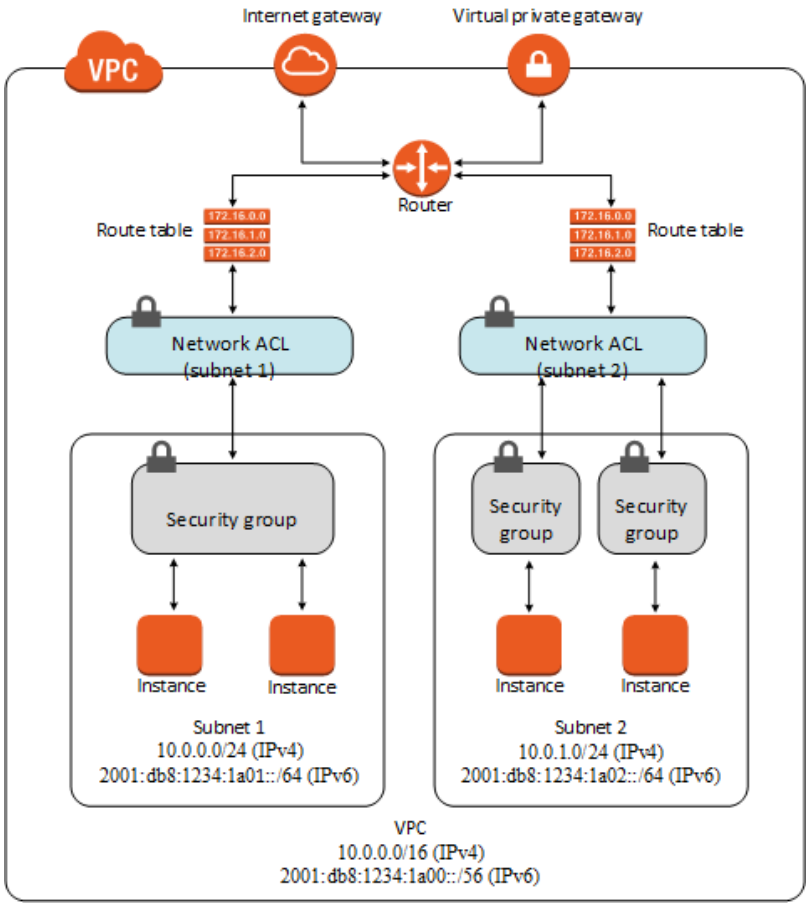
Three VPCs peered together



Route tables	Destination	Target
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-bbbbcccc
VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc
	10.0.0.0/16	pcx-bbbbcccc

Network ACL

protect your VPC
which control traffic in or out bound in VPC
by default all inbound and outbound traffic allow in default vpc
when we create a vpc one ACL is create in that ACL all inbound and outbound traffic allow
we create ACL and attach to VPC
we create acl all inbound and outbound traffic is deny
Each subnet in VPC associate with network ACL
when we create acl no subnet is associte
subnet is automatic associate with default network acl
network acl associate with multiple subnet
subnet is associate with only one network acl at a time
when we associate subnet to network acl at that time previous acl is remove
network acl have number of rules and rule number in multiple of 100
network acl are stateless
inbound and outbound have separate rules
security group for instance while network acl for subnet (vpc)



VPN connection

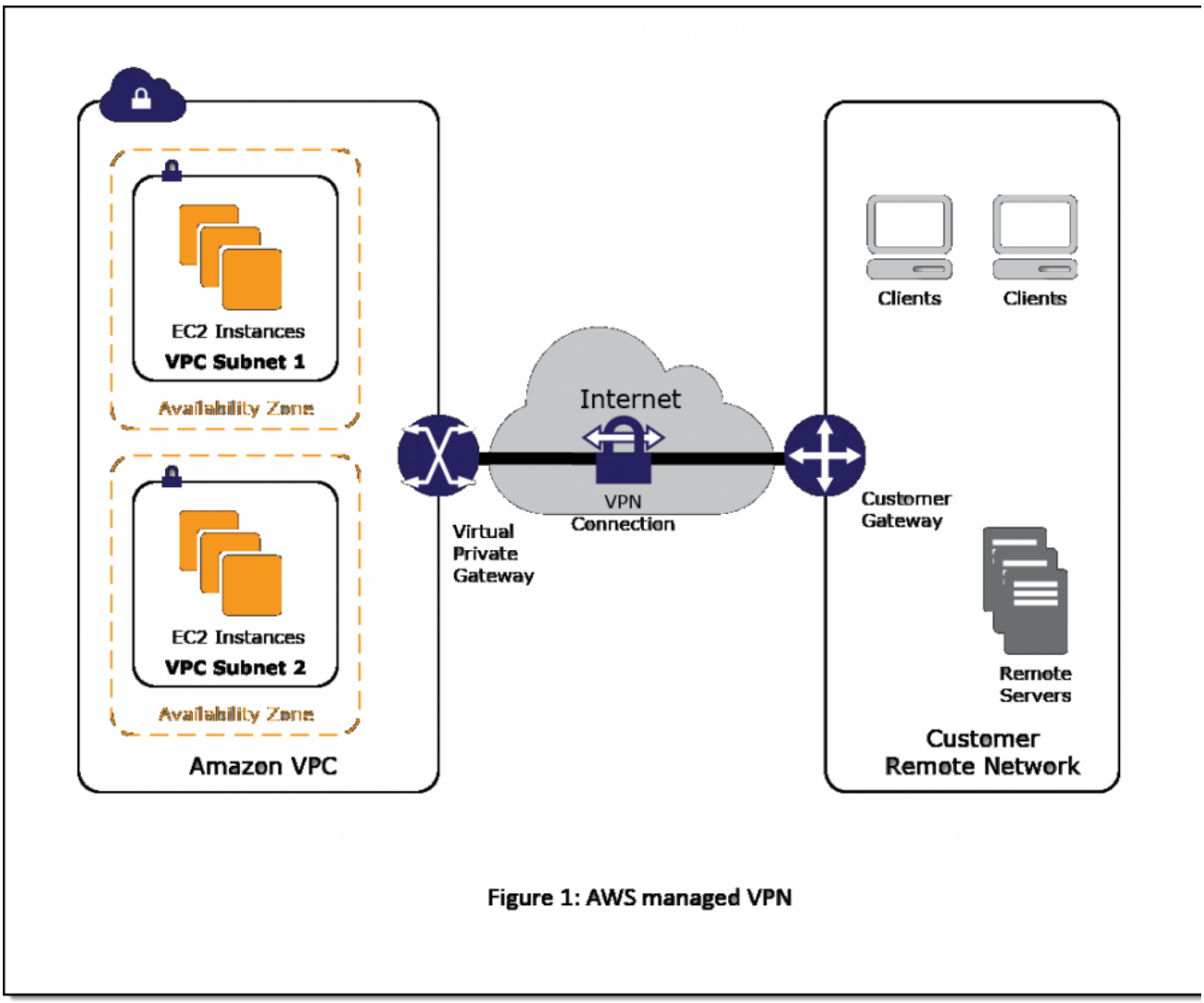


Figure 1: AWS managed VPN