

BRAINLY

MANAGING NETWORKING CHAOS WHILE MIGRATING TO AWS MULTI-ACCOUNT ARCHITECTURE

Routing in multi-account setup

26th November 2020

Agenda

1. About the presenter
2. Starting up with one account
3. Scaling up to few accounts
4. Further scaling to hundreds of accounts
5. Expanding to cross-region

WELCOME

Krzysztof Szyper

- Senior Infrastructure Engineer at Brainly
- Using AWS since 2012
- Everything-as-Code enthusiast
- <https://shyper.pro>



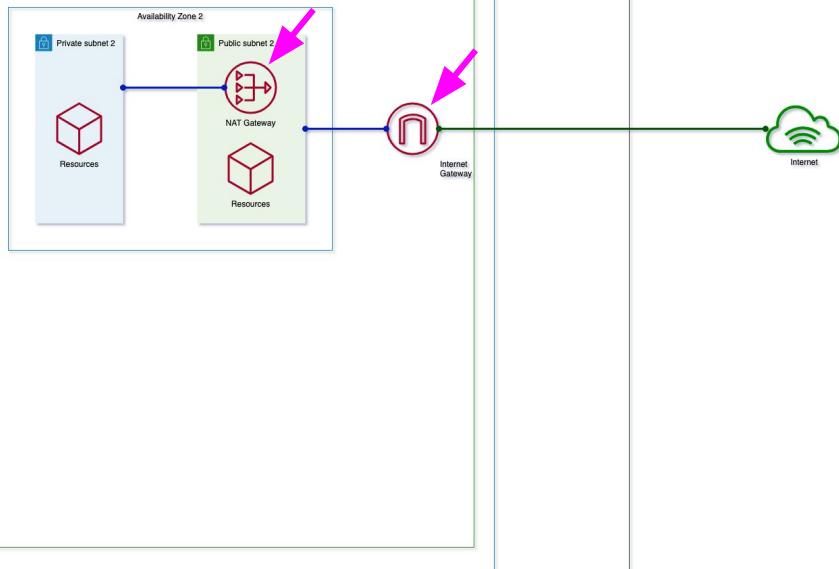
- All-to-all routing
- 3 AZs per VPC, only 4 VPCs per region,
only 2 regions
- Just some basic connections
- Only IPv4
- Split tunnel VPN, 8h/day/user
- Not calculating data transfer costs
- Cloud networks at 10.0.0.0/9,
Corporate networks at 10.128.0.0/9

Simplified setup

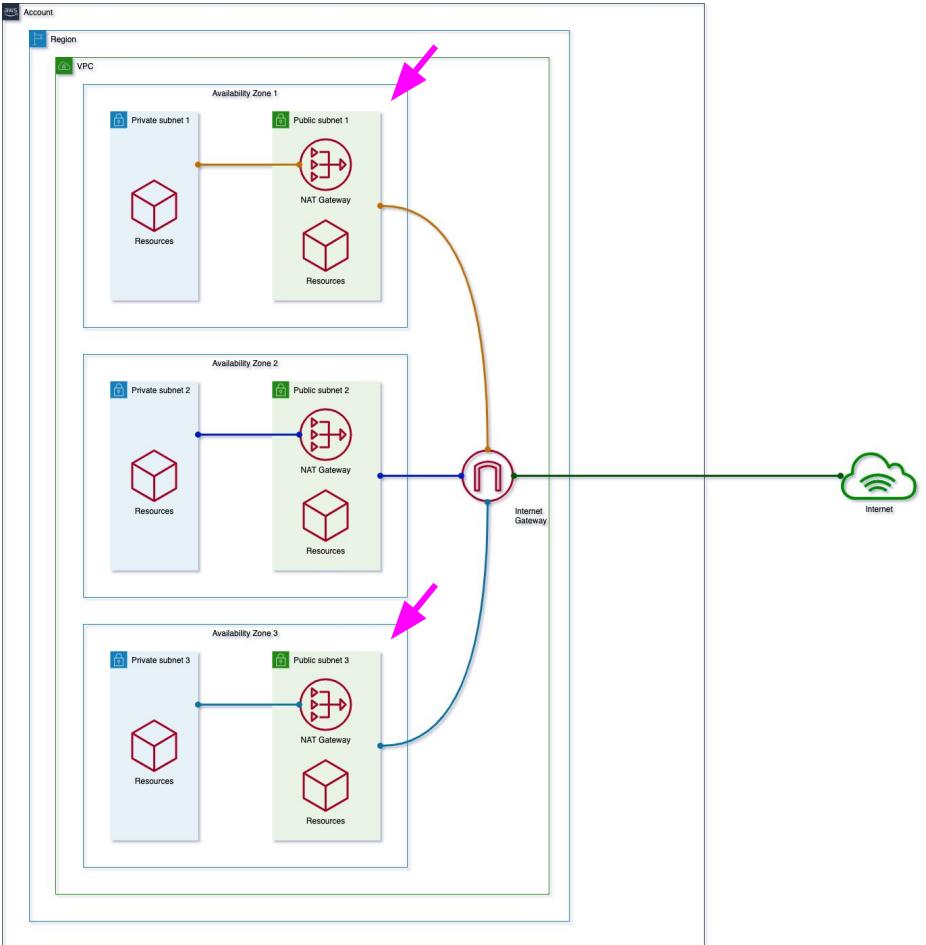
How do we start?

Let's begin with one VPC

Destination	Private	Public	VPE
10.0.0.0/16 (VPC)	Local	Local	-
0.0.0.0/0	nat-1a...	igw-1...	-

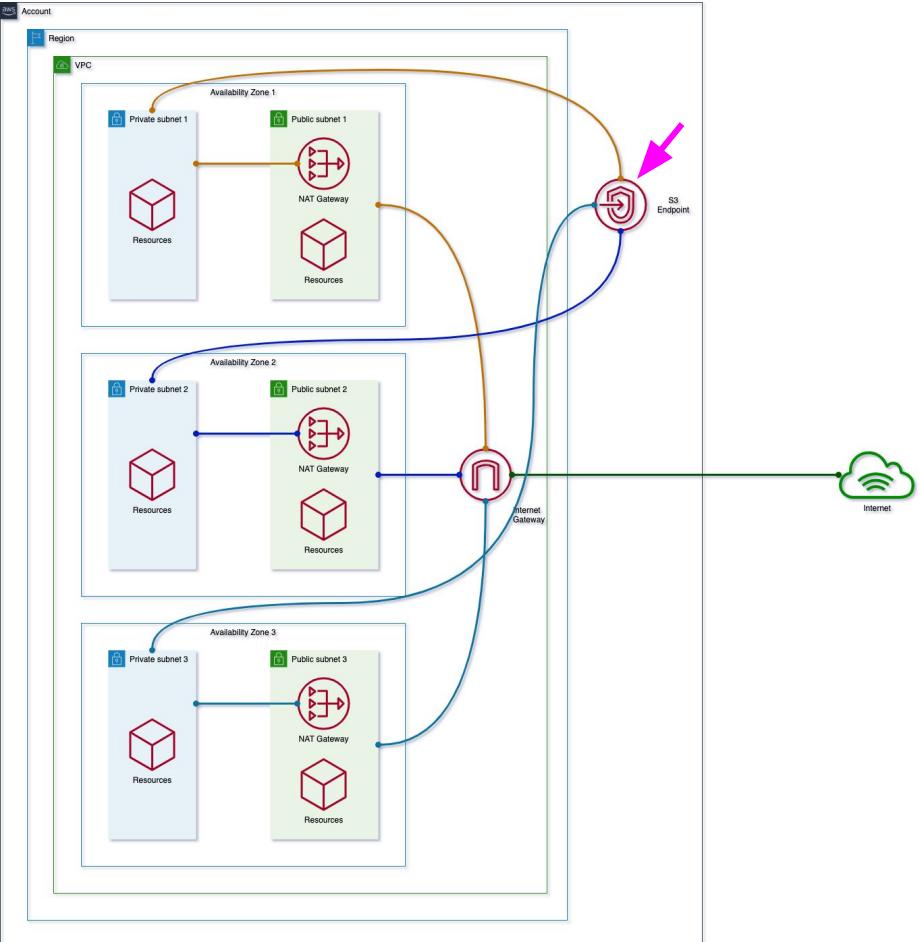


Resources	Costs
NAT GW	\$35 + data
IGW	data
VPE	-
VGW	-
Sum:	\$35 + data



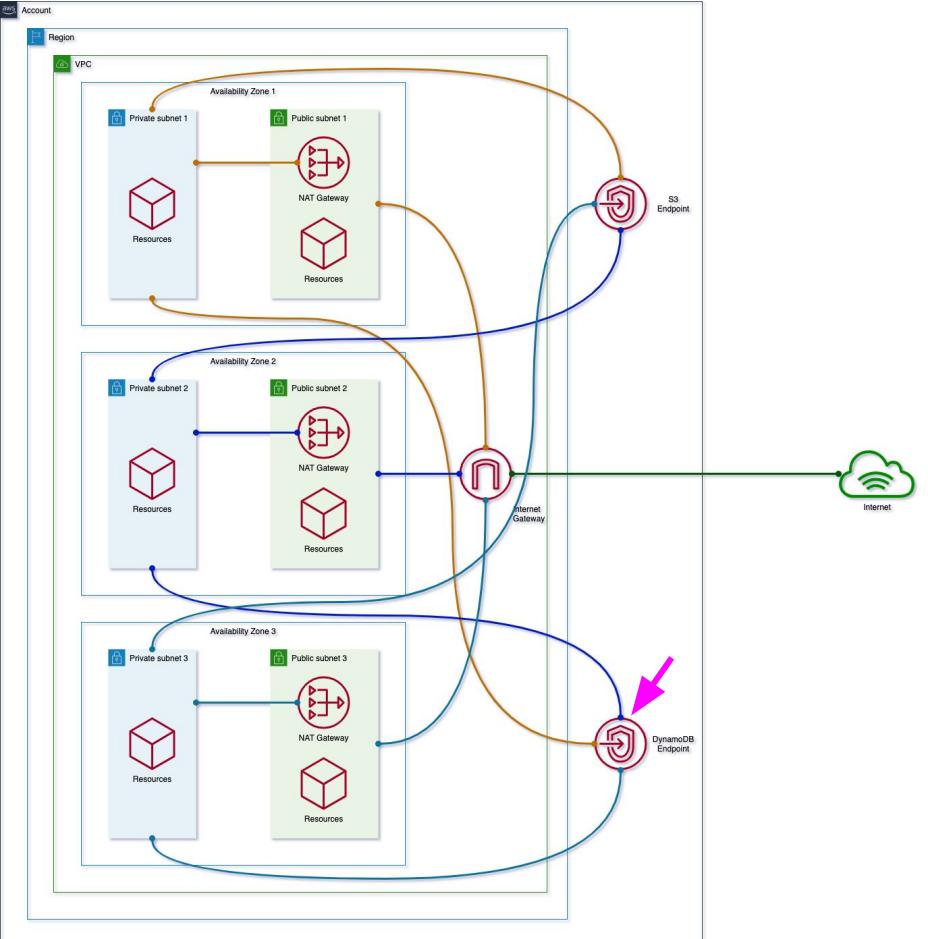
Destination	Private	Public	VPE
10.0.0.0/16 (VPC)	Local	Local	-
0.0.0.0/0	nat-1a... nat-1b... nat-1c...	igw-1...	-

Resources	Costs
NAT GW	\$35 + data + \$70 data
IGW	-
VPE	-
VGW	-
Sum:	\$105 + data



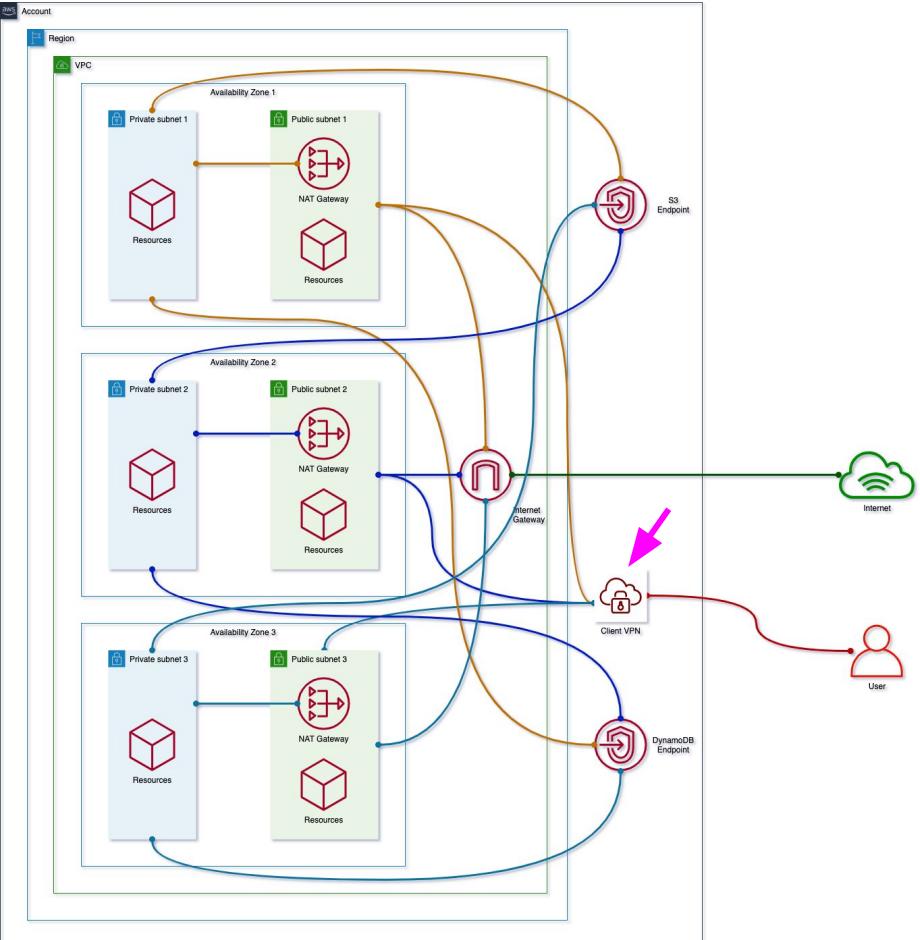
Destination	Private	Public	VPE
10.0.0.0/16 (VPC)	Local	Local	-
0.0.0.0/0	nat-1a... nat-1b... nat-1c...	igw-1...	-
pl-1a... (S3)	vpc-1a...	-	-

Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	-
VGW	-
Sum:	\$105 + data



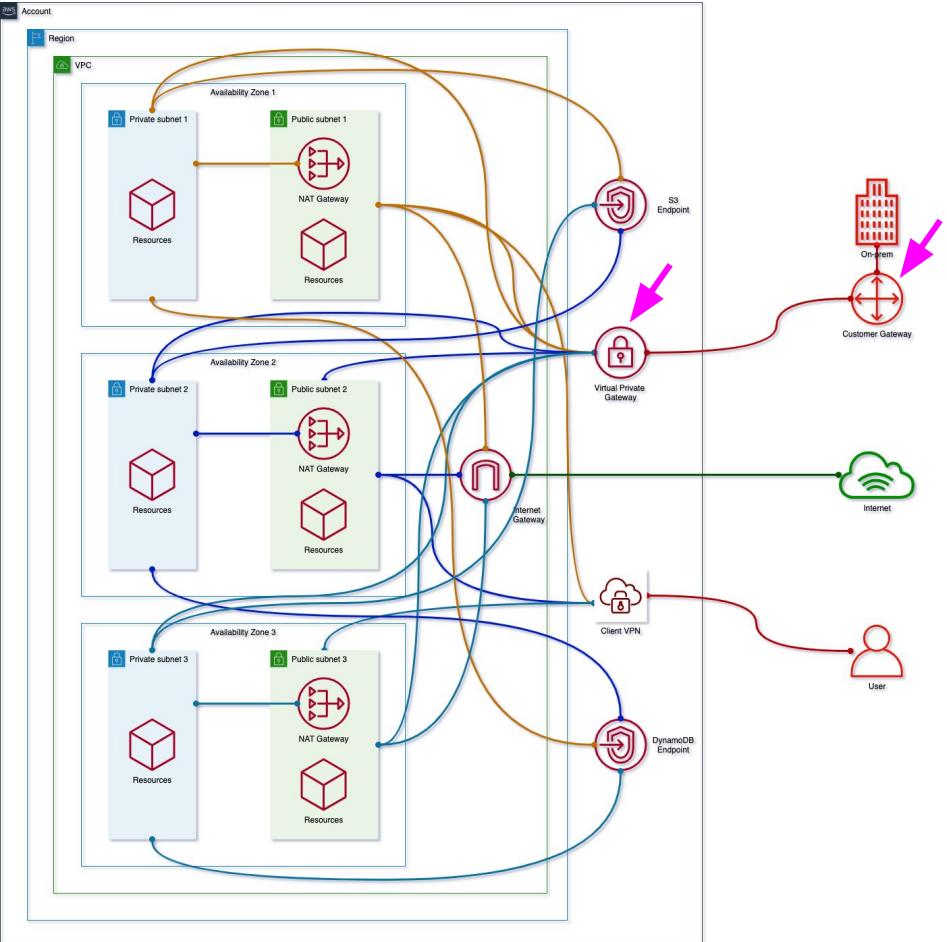
Destination	Private	Public	VPE
10.0.0.0/16 (VPC)	Local	Local	-
0.0.0.0/0	nat-1a... nat-1b... nat-1c...	igw-1...	-
pl-1a... (S3)	vpc-1a...	-	-
pl-1b... (DynamoDB)	vpc-1b...	-	-

Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	-
VGW	-
Sum:	\$105 + data



Destination	Private	Public	VPE
10.0.0.0/16 (VPC)	Local	Local	subnet-1a subnet-1b subnet-1c
0.0.0.0/0	nat-1a... nat-1b... nat-1c...	igw-1...	-
pl-1a... (S3) pl-1b... (DynDB)	vpc-1a... vpc-1b...	- -	- -
169.254.169.252 /30 (AWS)	-	-	subnet-1a subnet-1b subnet-1c

Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	\$36 + \$219 (assoc) + \$12 (user)
VGW	-
Sum:	\$360 + \$12/user + data

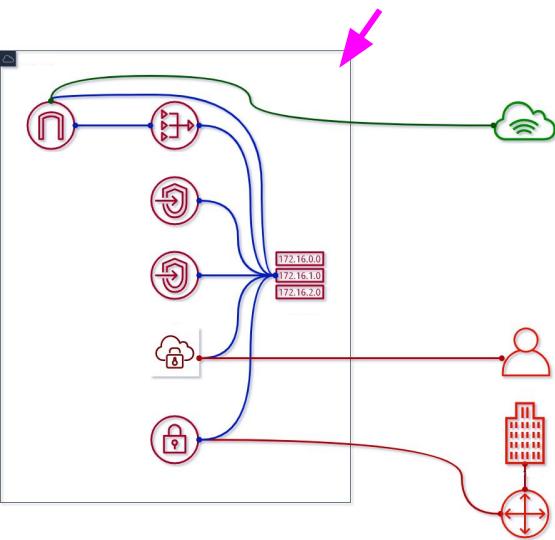


Destination	Private	Public	VPE
10.0.0.0/16 (VPC)	Local	Local	subnet-1a subnet-1b subnet-1c
0.0.0.0/0	nat-1a... nat-1b... nat-1c...	igw-1...	-
pl-1a... (S3) pl-1b... (DynDB)	vpc-1a... vpc-1b...	- -	- -
169.254.169.252 /30 (AWS)	-	-	subnet-1a subnet-1b subnet-1c
10.128.0.0/9 (Corp)	vgw-1...	vgw-1...	subnet-1a subnet-1b subnet-1c

Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
Sum:	\$396 + \$12/user + data

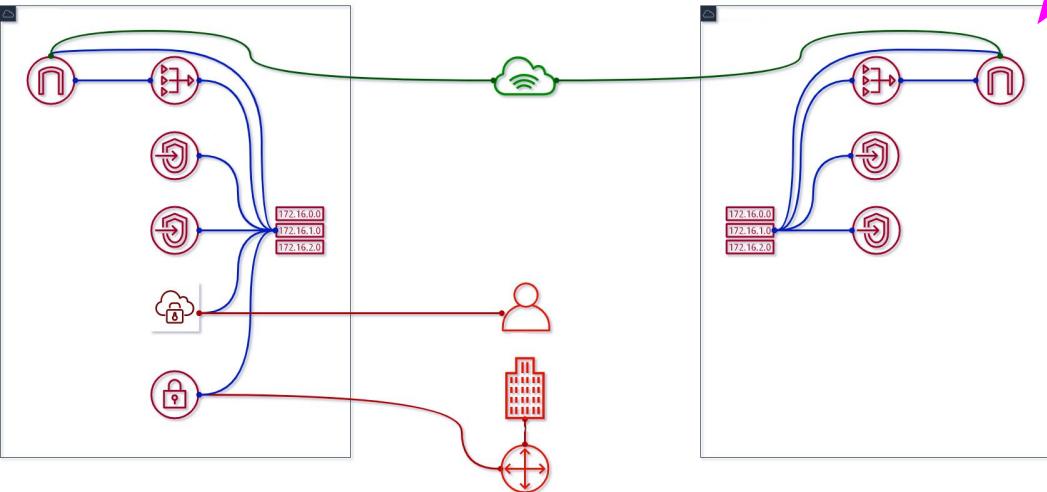
How can we expand?

Now add few more VPCs and peer them



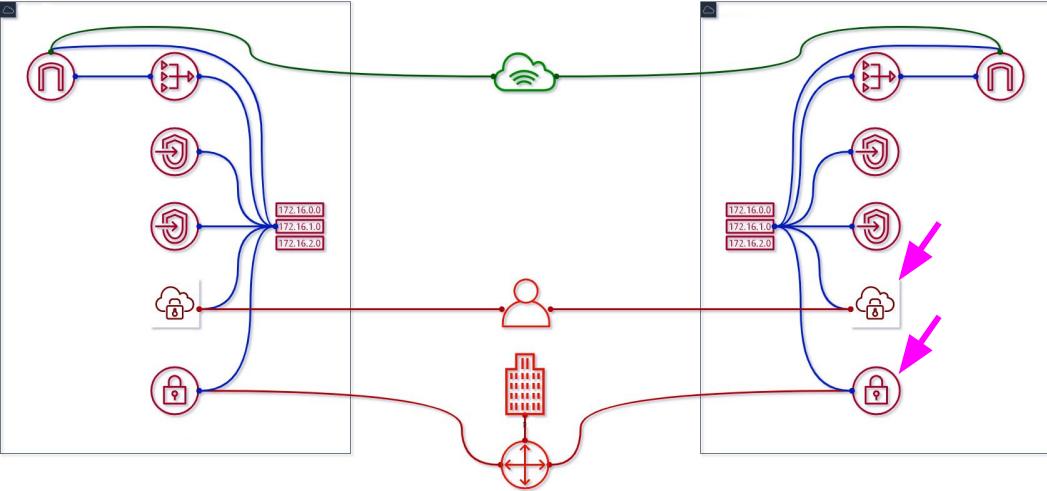
Destination	Private	Public	VPE
10.0.0.0/16 (VPC)	Local	Local	
0.0.0.0/0	nat-1a/b/c...	igw-1...	-
pl-1a... (S3)	vpc-1a...	-	-
pl-1b... (DynDB)	vpc-1b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1...	vgw-1...	subnet-1a/b/c

Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
Sum:	\$396 + \$12/user + data



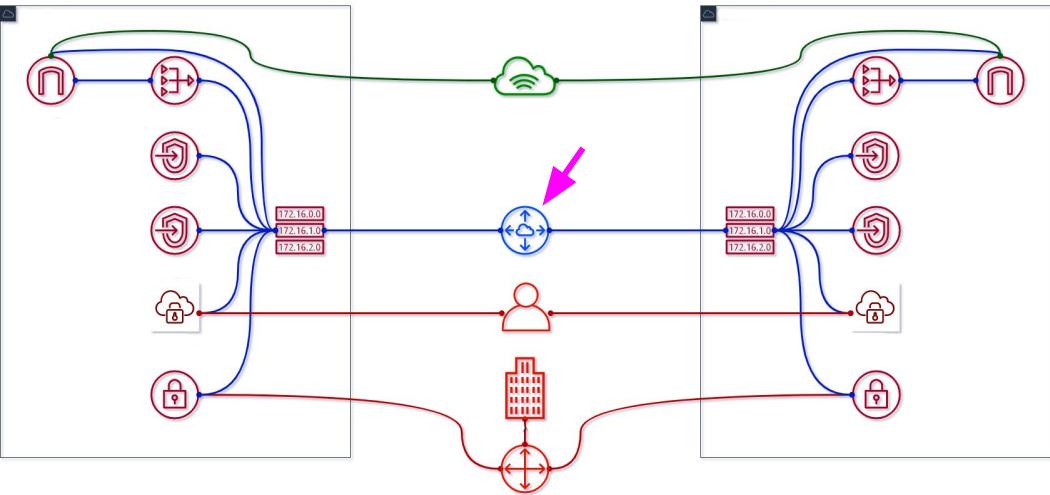
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)	nat-1a/b/c...	igw-1...	-
0.0.0.0/0	nat-2a/b/c...	igw-2...	-
pl... (S3)	vpc-1a...	-	-
pl... (DynamoDB)	vpc-2a...	-	-
vpc-1b...		-	-
169.254.169.252 /30 (AWS)		-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1...	vgw-1...	subnet-1a/b/c

Resources	Costs
NAT GW	\$105 + data + \$105
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
Sum:	\$501 + \$12/user + data



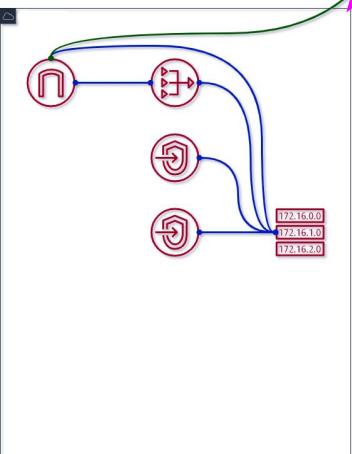
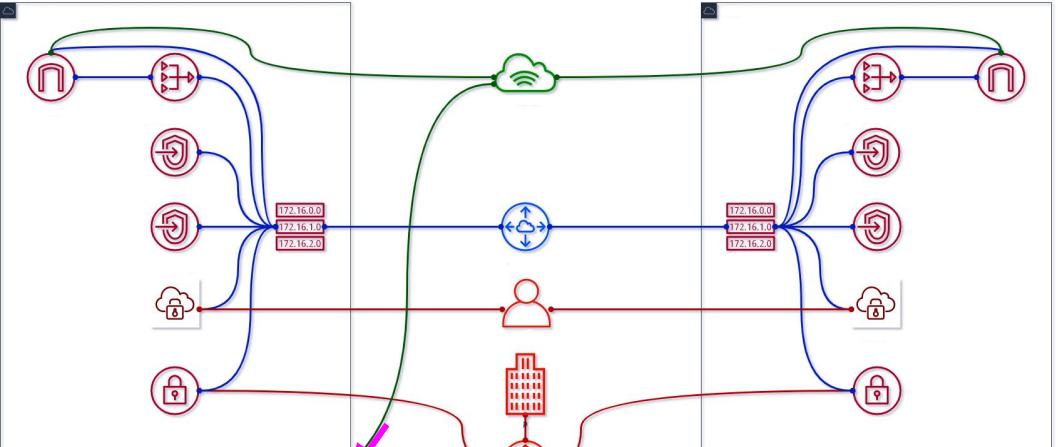
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c...	igw-1... igw-2...	-
pl-... (S3)	vpc-1a... vpc-2a...	-	-
pl-... (DynDB)	vpc-1b... vpc-2b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2...	vgw-1... vgw-2...	subnet-1a/b/c subnet-2a/b/c

Resources	Costs
NAT GW	\$210 + data
IGW	data
VPE	\$255 + \$12 (user) + \$255
VGW	\$36 + \$36
Sum:	\$792 + \$12/user + data



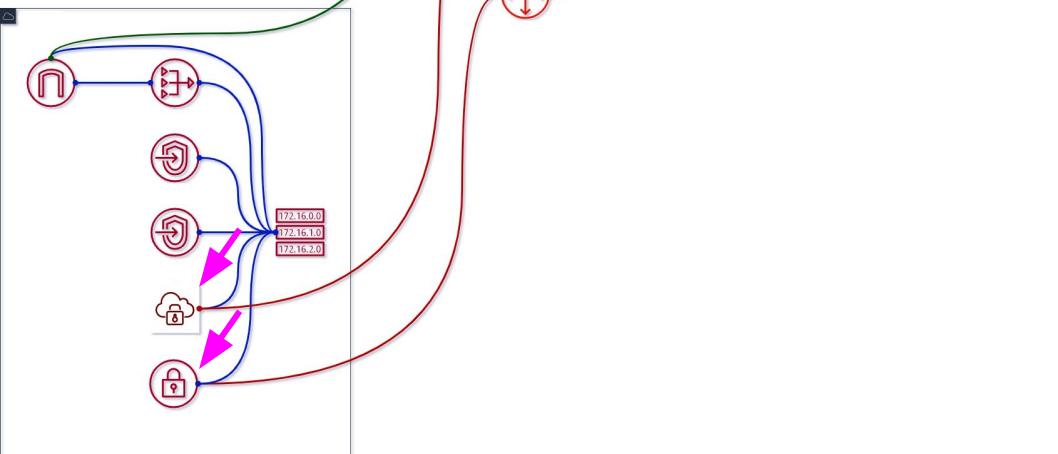
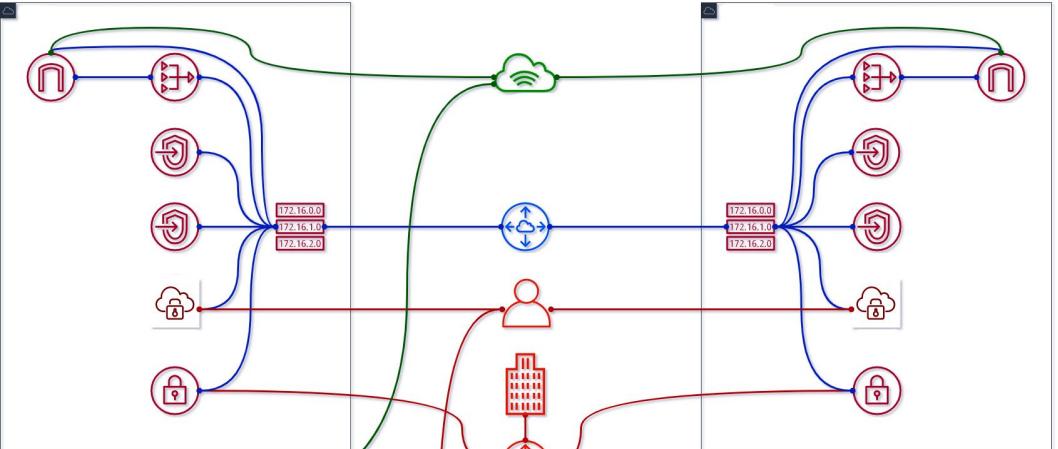
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c...	igw-1... igw-2...	-
pl-... (S3)	vpc-1a... vpc-2a...	-	-
pl-... (DynamoDB)	vpc-1b... vpc-2b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2...	vgw-1... vgw-2...	subnet-1a/b/c subnet-2a/b/c
10.0.0.0/16 (VPC1)	pcx-2...	pcx-2...	-
10.1.0.0/16 (VPC2)	pcx-1...	pcx-1...	-

Resources	Costs
NAT GW	\$210 + data
IGW	data
VPE	\$510 + \$12 (user)
VGW	\$72
Sum:	\$792 + \$12/user + data



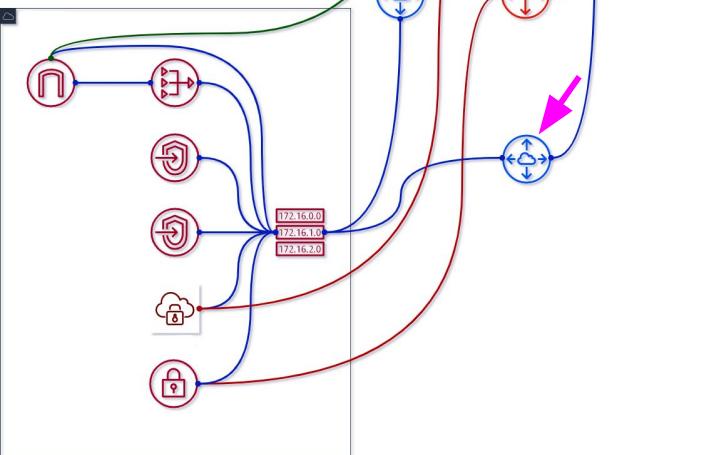
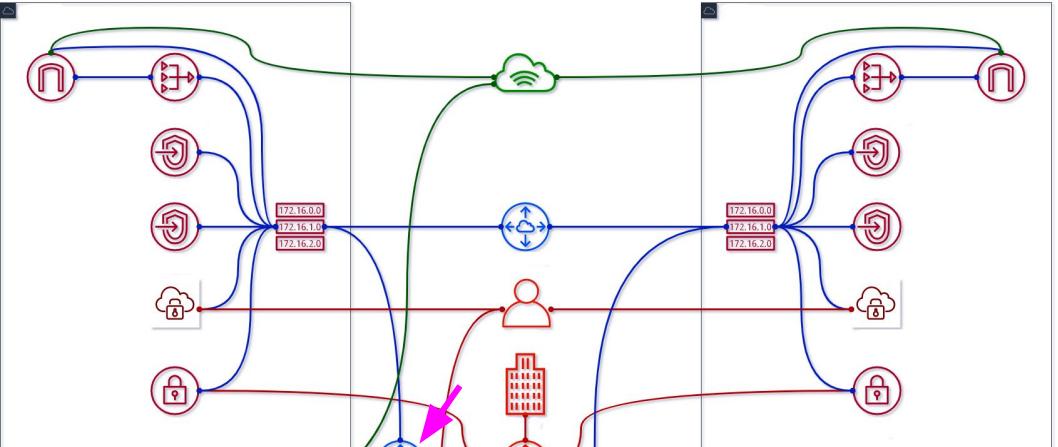
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
10.2.0.0/16 (VPC3)			
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c...	igw-1... igw-2... igw-3...	-
pl... (S3)	vpc-1a/2a/3a...	-	-
pl... (DynDB)	vpc-1b/2b/3b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2...	vgw-1... vgw-2...	subnet-1a/b/c subnet-2a/b/c
10.0.0.0/16 (VPC1)	pcx-2...	pcx-2...	-
10.1.0.0/16 (VPC2)	pcx-1...	pcx-1...	-

Resources	Costs
NAT GW	\$210 + data + \$105
IGW	data
VPE	\$510 + \$12 (user)
VGW	\$72
Sum:	\$897 + \$12/user + data



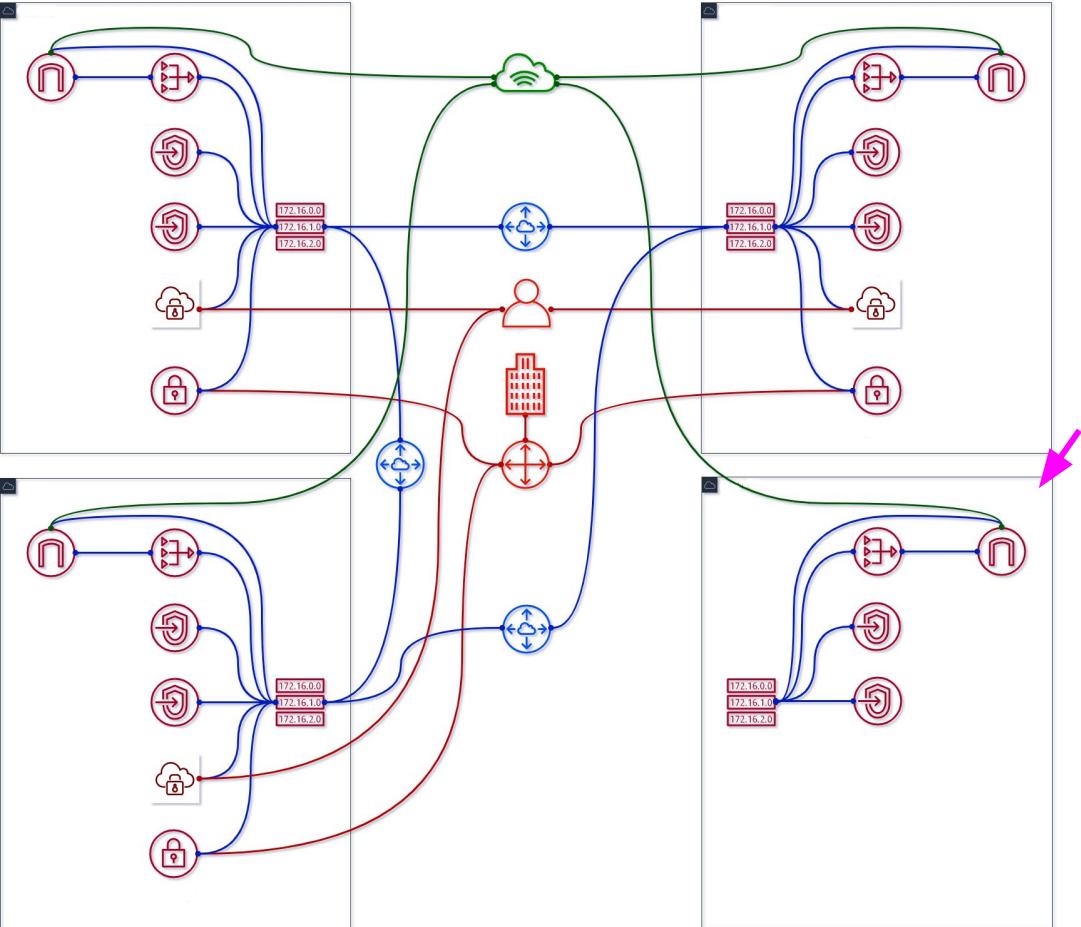
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
10.2.0.0/16 (VPC3)			subnet-3a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c...	igw-1... igw-2... igw-3...	-
pl... (S3)	vpc-1a/2a/3a...	-	-
pl... (DynDB)	vpc-1b/2b/3b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3...	vgw-1... vgw-2... vgw-3...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c
10.0.0.0/16 (VPC1)	pcx-2...	pcx-2...	-
10.1.0.0/16 (VPC2)	pcx-1...	pcx-1...	-

Resources	Costs
NAT GW	\$315 + data
IGW	data
VPE	\$510 + \$12 (user) + \$255
VGW	\$72 + \$36
Sum:	\$1188 + \$12/user + data



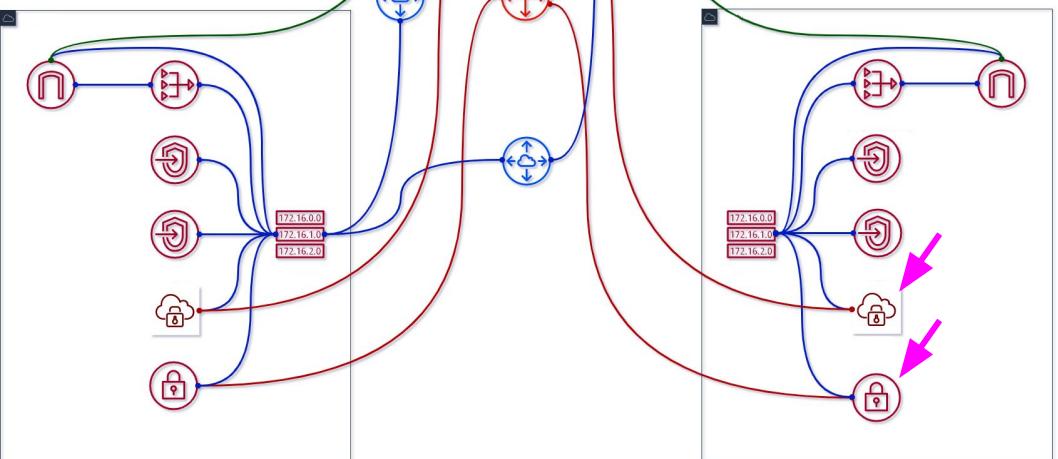
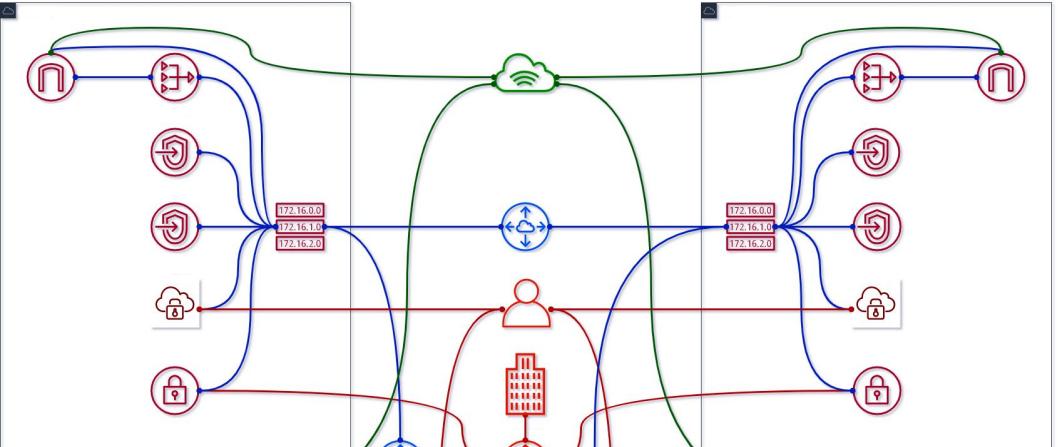
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
10.2.0.0/16 (VPC3)			subnet-3a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c...	igw-1... igw-2... igw-3...	-
pl... (S3)	vpc-1a/2a/3a...	-	-
pl... (DynDB)	vpc-1b/2b/3b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3...	vgw-1... vgw-2... vgw-3...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c
10.0.0.0/16 (VPC1)	pcx-2/3...	pcx-2/3...	-
10.1.0.0/16 (VPC2)	pcx-1/3...	pcx-1/3...	-
10.2.0.0/16 (VPC3)	pcx-1/2...	pcx-1/2...	-

Resources	Costs
NAT GW	\$315 + data
IGW	data
VPE	\$765 + \$12 (user)
VGW	\$108
Sum:	\$1188 + \$12/user + data



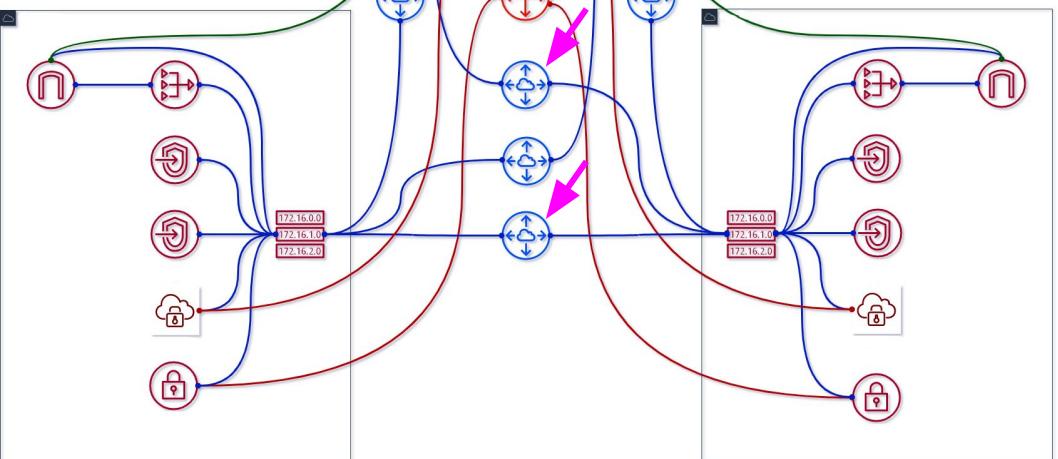
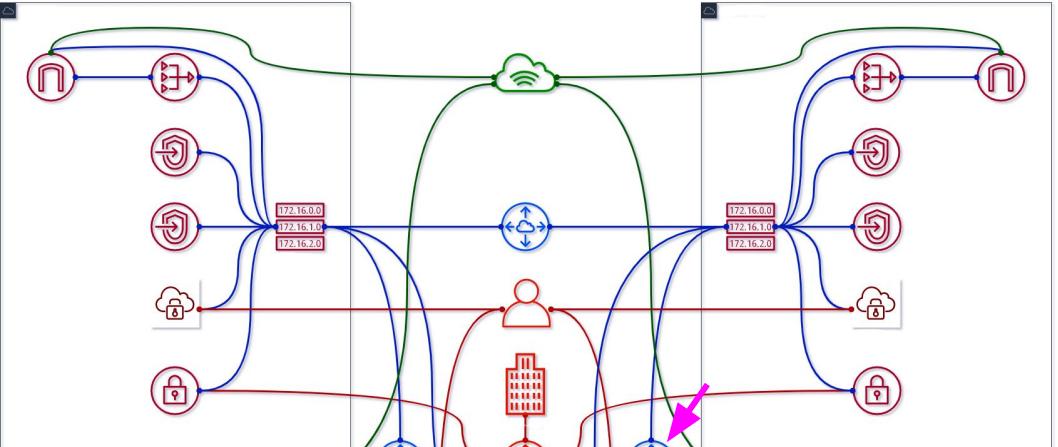
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
10.2.0.0/16 (VPC3)			subnet-3a/b/c
10.3.0.0/16 (VPC4)			
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-1... igw-2... igw-3... igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3...	vgw-1... vgw-2... vgw-3...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c
10.0.0.0/16 (VPC1)	pcx-2/3...	pcx-2/3...	-
10.1.0.0/16 (VPC2)	pcx-1/3...	pcx-1/3...	-
10.2.0.0/16 (VPC3)	pcx-1/2...	pcx-1/2...	-

Resources	Costs
NAT GW	\$315 + data + \$105
IGW	data
VPE	\$765 + \$12 (user)
VGW	\$108
Sum:	\$1293 + \$12/user + data



Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)		igw-1...	subnet-2a/b/c
10.2.0.0/16 (VPC3)		igw-2...	subnet-3a/b/c
10.3.0.0/16 (VPC4)		igw-3...	subnet-4a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3... vgw-4...	vgw-1... vgw-2... vgw-3... vgw-4...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-2/3...	pcx-2/3...	-
10.1.0.0/16 (VPC2)	pcx-1/3...	pcx-1/3...	-
10.2.0.0/16 (VPC3)	pcx-1/2...	pcx-1/2...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$765 + \$12 (user) + \$255
VGW	\$108 + \$36
Sum:	\$1584 + \$12/user + data

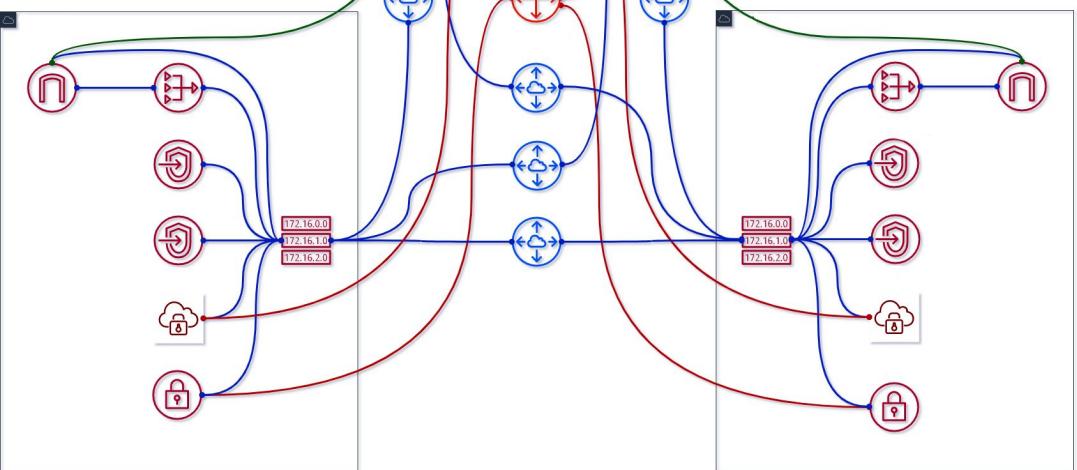
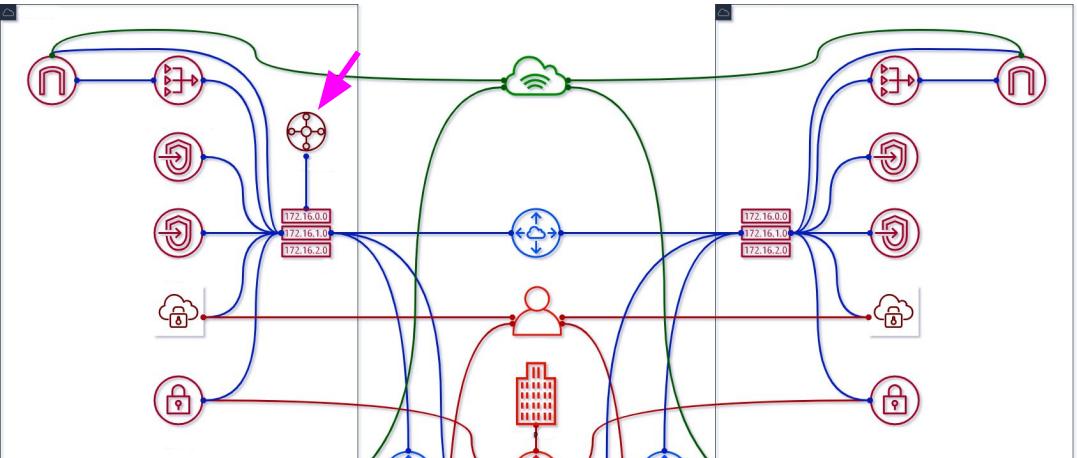


Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)		igw-1...	subnet-2a/b/c
10.2.0.0/16 (VPC3)		igw-2...	subnet-3a/b/c
10.3.0.0/16 (VPC4)		igw-3...	subnet-4a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3... vgw-4...	vgw-1... vgw-2... vgw-3... vgw-4...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-2/3/4...	pcx-2/3/4...	-
10.1.0.0/16 (VPC2)	pcx-1/3/4...	pcx-1/3/4...	-
10.2.0.0/16 (VPC3)	pcx-1/2/4...	pcx-1/2/4...	-
10.3.0.0/16 (VPC4)	pcx-1/2/3...	pcx-1/2/3...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$1020 + \$12 (user)
VGW	\$144
Sum:	\$1584 + \$12/user + data

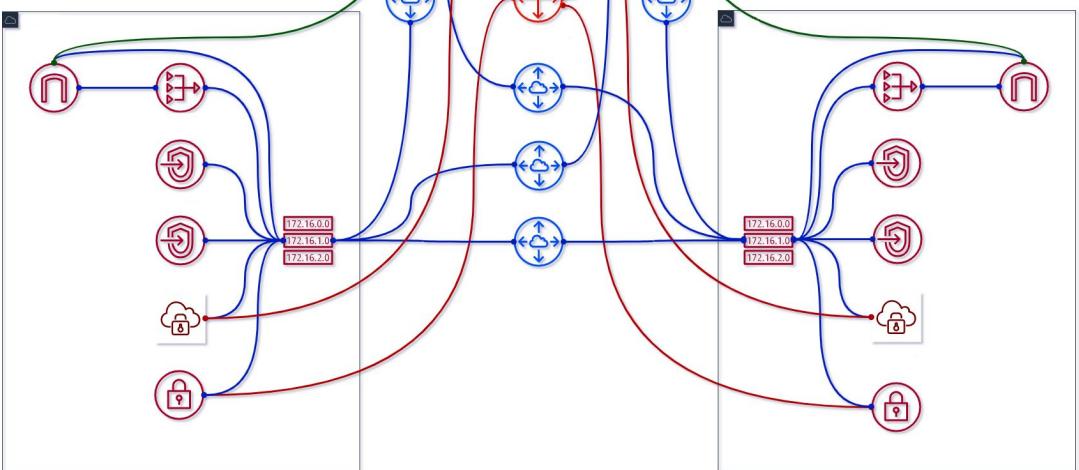
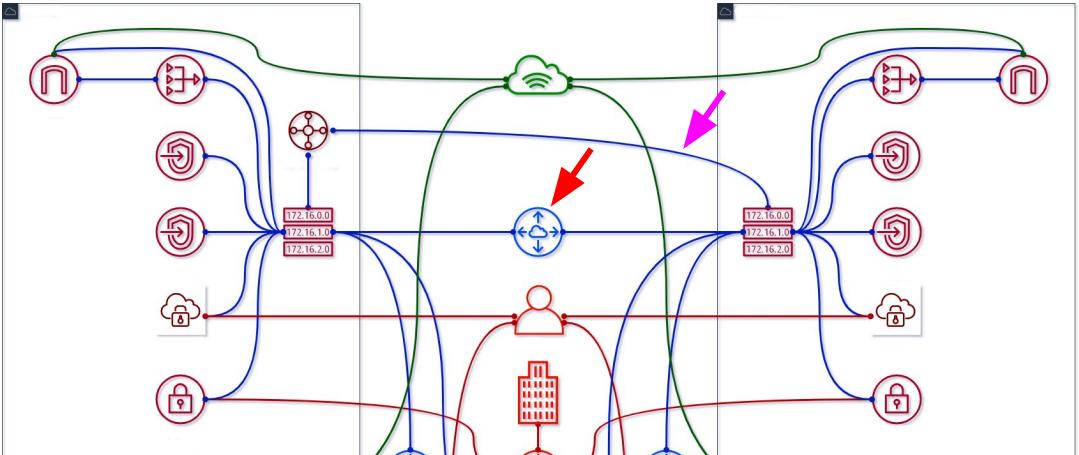
Can we grow further?

Add even more VPCs with Transit Gateway



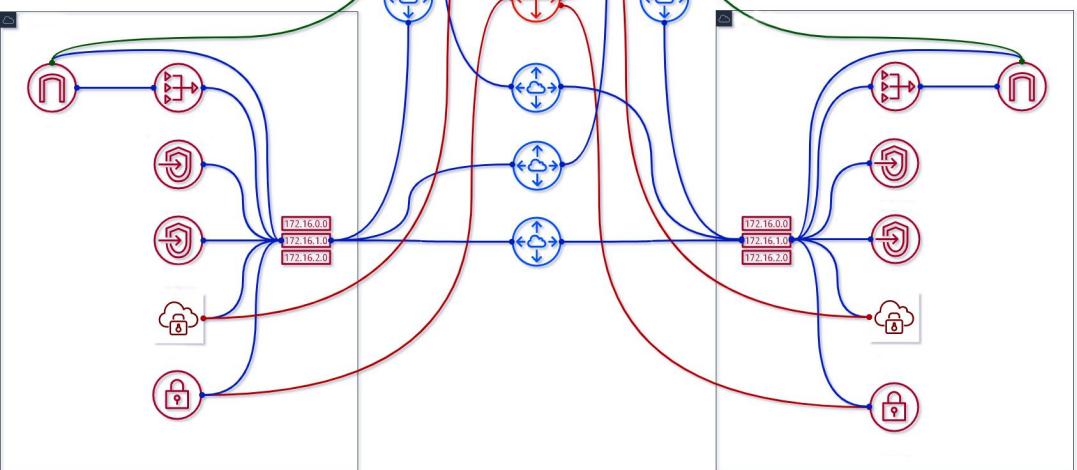
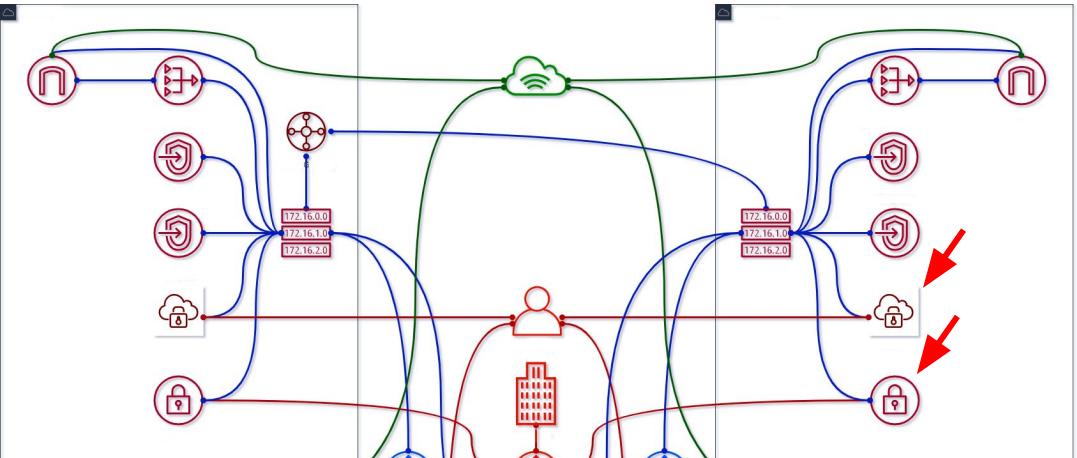
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)		igw-1...	subnet-2a/b/c
10.2.0.0/16 (VPC3)		igw-2...	subnet-3a/b/c
10.3.0.0/16 (VPC4)		igw-3...	subnet-4a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3... vgw-4...	vgw-1... vgw-2... vgw-3... vgw-4...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-2/3/4...	pcx-2/3/4...	-
10.1.0.0/16 (VPC2)	pcx-1/3/4...	pcx-1/3/4...	-
10.2.0.0/16 (VPC3)	pcx-1/2/4...	pcx-1/2/4...	-
10.3.0.0/16 (VPC4)	pcx-1/2/3...	pcx-1/2/3...	-
10.0.0.0/9 (Cloud)	tgw-att-1...	tgw-att-1...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$1020 + \$12 (user)
VGW	\$144
TGW	\$36 + data
Sum:	\$1620 + \$12/user + data



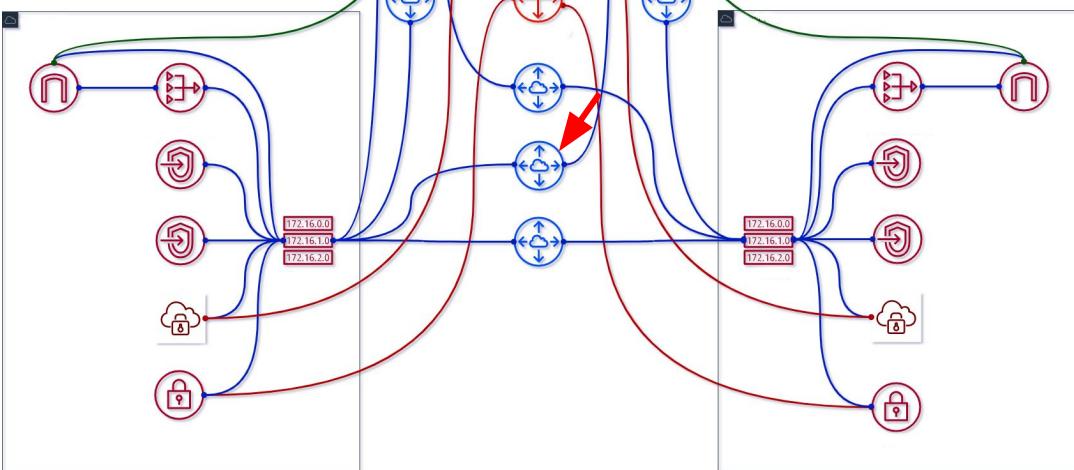
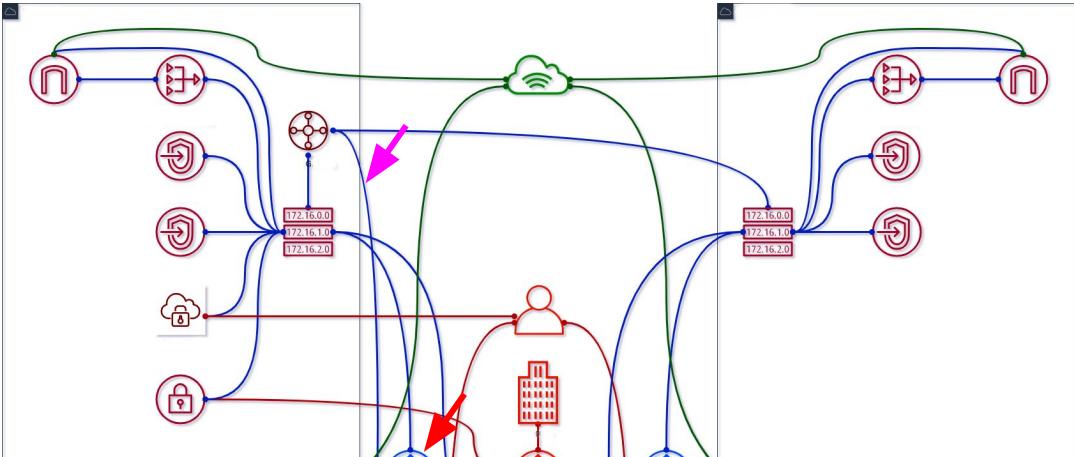
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
10.2.0.0/16 (VPC3)			subnet-3a/b/c
10.3.0.0/16 (VPC4)			subnet-4a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-1... igw-2... igw-3... igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3... vgw-4...	vgw-1... vgw-2... vgw-3... vgw-4...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-2/3/4...	pcx-2/3/4...	-
10.1.0.0/16 (VPC2)	pcx-1/3/4...	pcx-1/3/4...	-
10.2.0.0/16 (VPC3)	pcx-1/2/4...	pcx-1/2/4...	-
10.3.0.0/16 (VPC4)	pcx-1/2/3...	pcx-1/2/3...	-
10.0.0.0/9 (Cloud)	tgw-att-1/2...	tgw-att-1/2...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$1020 + \$12 (user)
VGW	\$144
TGW	\$36 + data + \$36
Sum:	\$1656 + \$12/user + data



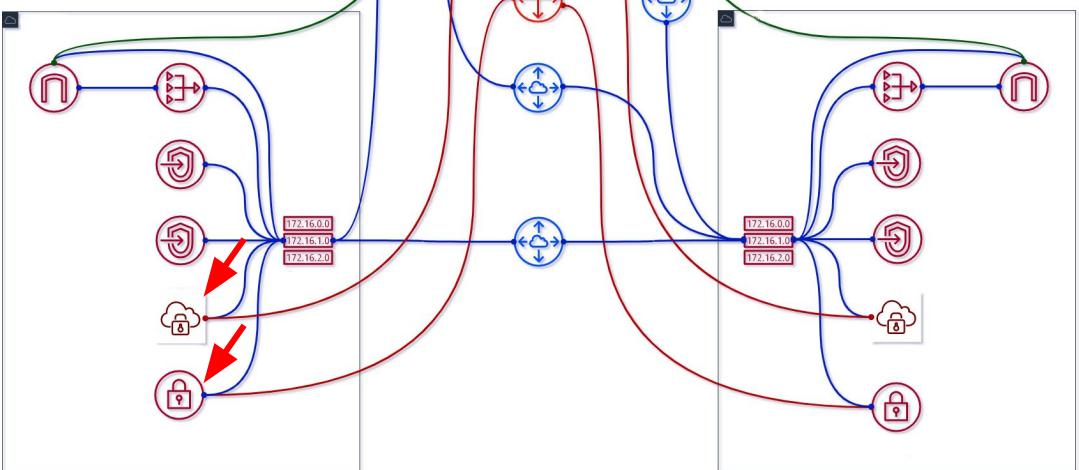
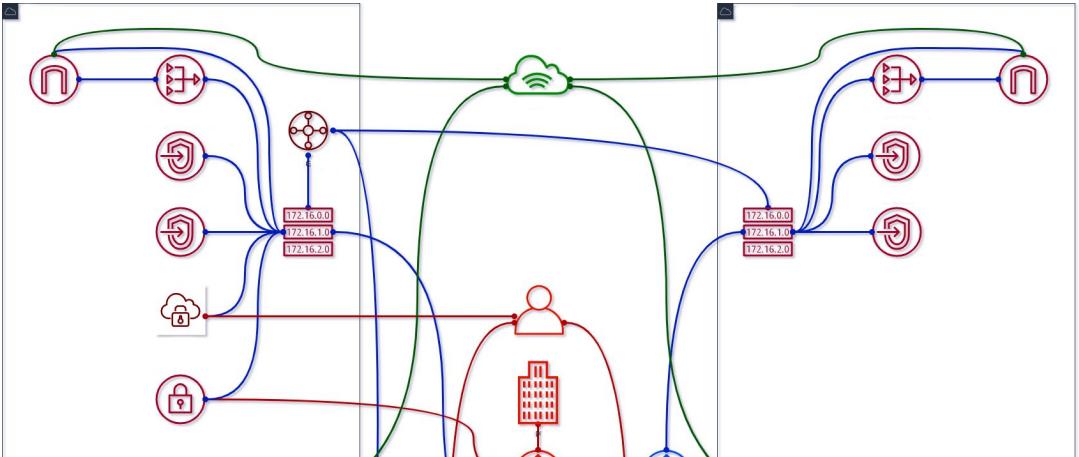
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-2a/b/c
10.2.0.0/16 (VPC3)			subnet-3a/b/c
10.3.0.0/16 (VPC4)			subnet-4a/b/c
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-1... igw-2... igw-3... igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-2... vgw-3... vgw-4... tgw-att-2...	vgw-1... vgw-2... vgw-3... vgw-4... tgw-att-2...	subnet-1a/b/c subnet-2a/b/c subnet-3a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-3/4...	pcx-3/4...	-
10.1.0.0/16 (VPC2)	pcx-3/4...	pcx-3/4...	-
10.2.0.0/16 (VPC3)	pcx-1/2/4...	pcx-1/2/4...	-
10.3.0.0/16 (VPC4)	pcx-1/2/3...	pcx-1/2/3...	-
10.0.0.0/9 (Cloud)	tgw-att-1/2...	tgw-att-1/2...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$1020 + \$12 (user) - \$255
VGW	\$144 - \$36
TGW	\$72 + data
Sum:	\$1656 + \$12/user + data



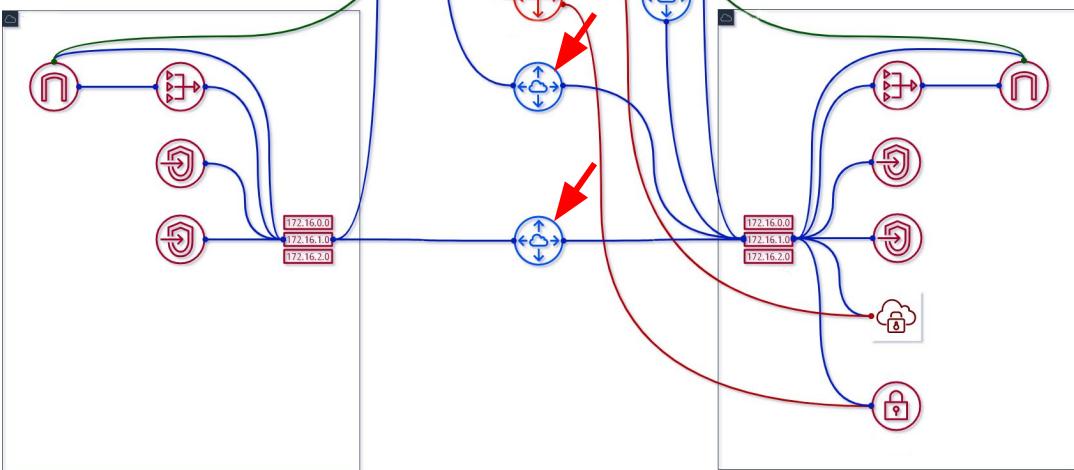
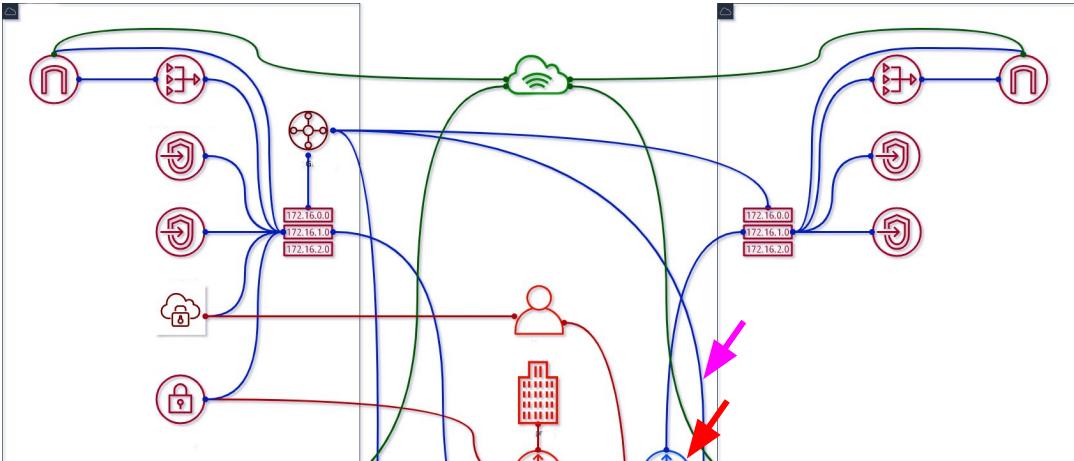
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-3a/b/c
10.2.0.0/16 (VPC3)			subnet-4a/b/c
10.3.0.0/16 (VPC4)			
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-1... igw-2... igw-3... igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-3a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-3... vgw-4... tgw-att-2...	vgw-1... vgw-3... vgw-4... tgw-att-2...	subnet-1a/b/c subnet-3a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-3/4...	pcx-3/4...	-
10.1.0.0/16 (VPC2)	pcx-3/4...	pcx-3/4...	-
10.2.0.0/16 (VPC3)	pcx-1/2/4...	pcx-1/2/4...	-
10.3.0.0/16 (VPC4)	pcx-1/2/3...	pcx-1/2/3...	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3...	tgw-att-1/2/3...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$765 + \$12 (user)
VGW	\$108
TGW	\$72 + data + \$36
Sum:	\$1401 + \$12/user + data



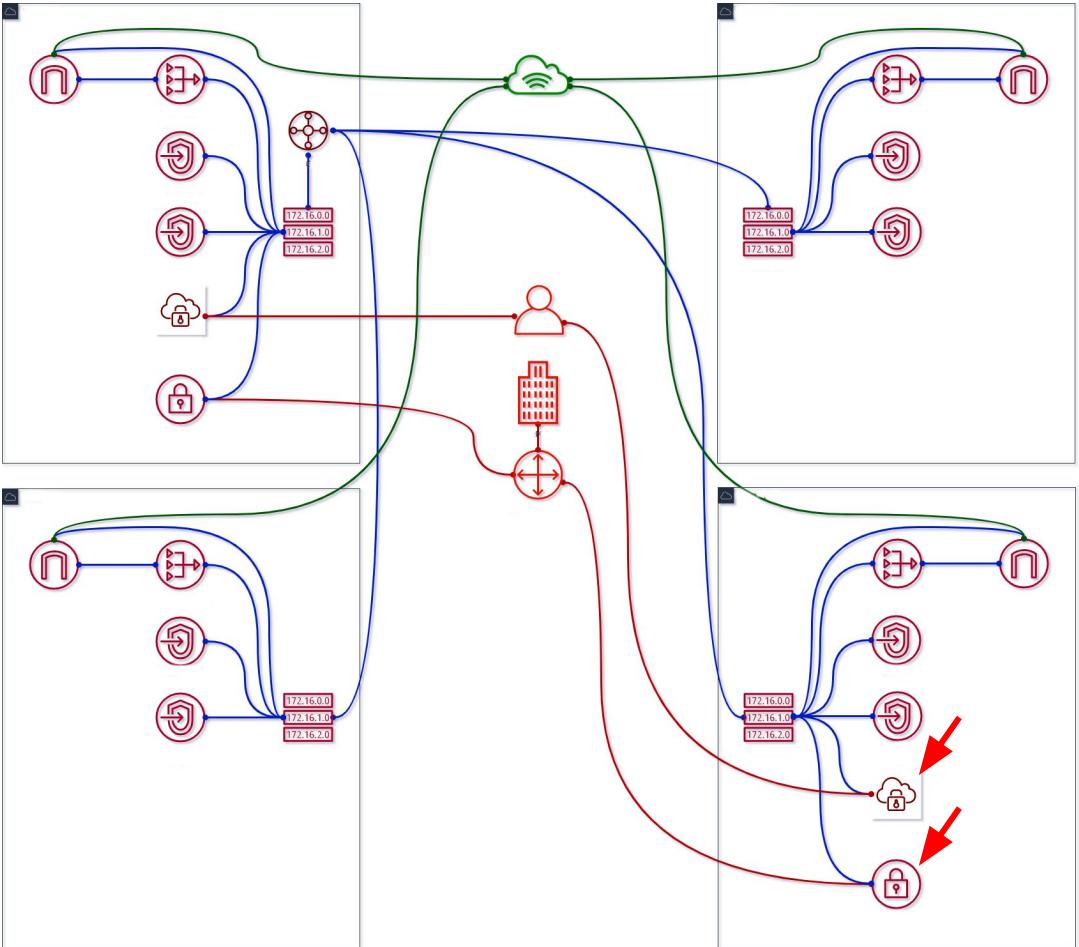
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)			subnet-3a/b/c
10.2.0.0/16 (VPC3)			subnet-4a/b/c
10.3.0.0/16 (VPC4)			
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-1... igw-2... igw-3... igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-3a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-3... vgw-4... tgw-att-2/3...	vgw-1... vgw-3... vgw-4... tgw-att-2/3...	subnet-1a/b/c subnet-3a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-4...	pcx-4...	-
10.1.0.0/16 (VPC2)	pcx-4...	pcx-4...	-
10.2.0.0/16 (VPC3)	pcx-4...	pcx-4...	-
10.3.0.0/16 (VPC4)	pcx-1/2/3...	pcx-1/2/3...	-
10.0.0.9 (Cloud)	tgw-att-1/2/3...	tgw-att-1/2/3...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$765 + \$12 (user) - \$255
VGW	\$108 - \$36
TGW	\$108 + data
Sum:	\$1401 + \$12/user + data



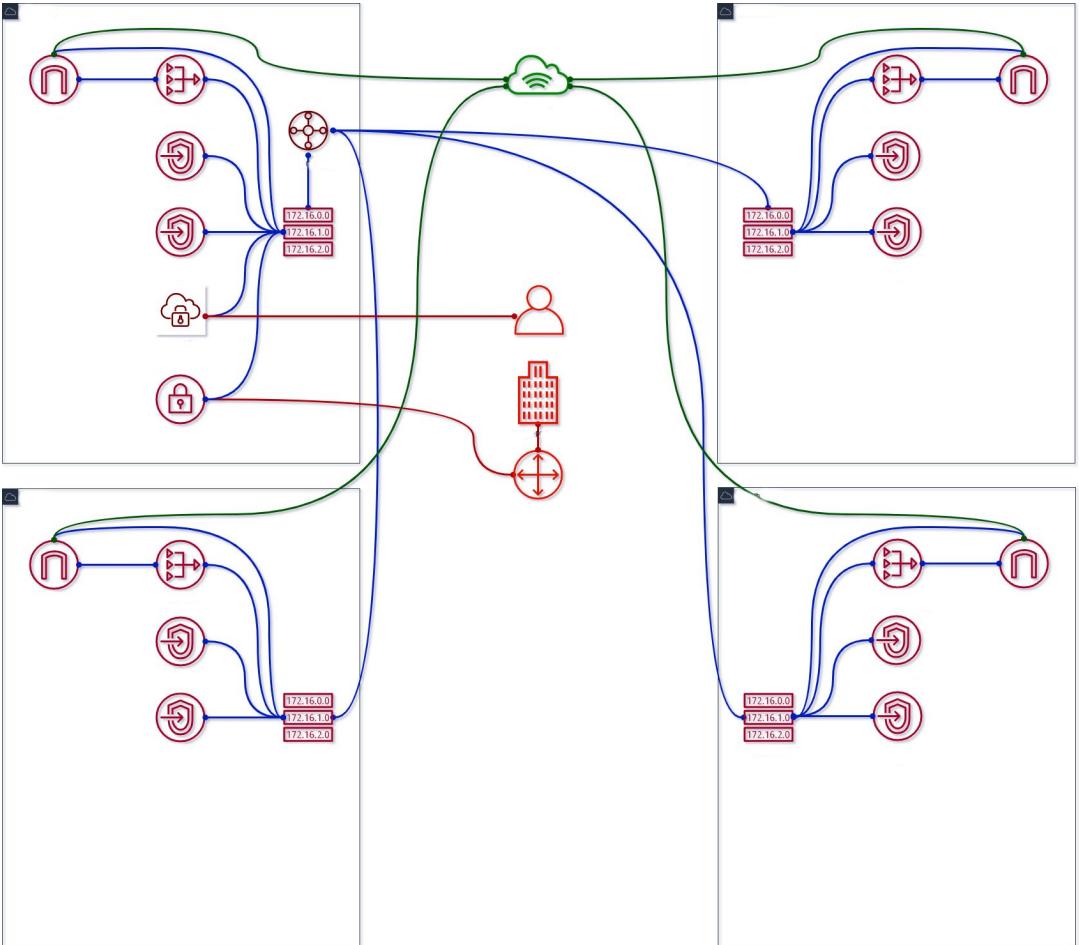
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)		igw-1...	
10.2.0.0/16 (VPC3)		igw-2...	
10.3.0.0/16 (VPC4)		igw-3...	
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-4... tgw-2/3...	vgw-1... vgw-4... tgw-2/3...	subnet-1a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	pcx-4...	pcx-4...	-
10.1.0.0/16 (VPC2)	pcx-4...	pcx-4...	-
10.2.0.0/16 (VPC3)	pcx-4...	pcx-4...	-
10.3.0.0/16 (VPC4)	pcx-1/2/3...	pcx-1/2/3...	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$510 + \$12 (user)
VGW	\$72
TGW	\$108 + data + \$36
Sum:	\$1146 + \$12/user + data



Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)		igw-1...	subnet-4a/b/c
10.2.0.0/16 (VPC3)		igw-2...	
10.3.0.0/16 (VPC4)		igw-3...	
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-4a/b/c
10.128.0.0/9 (Corp)	vgw-1... vgw-4... tgw-2/3/4...	vgw-1... vgw-4... tgw-2/3/4...	subnet-1a/b/c subnet-4a/b/c
10.0.0.0/16 (VPC1)	-	-	-
10.1.0.0/16 (VPC2)	-	-	-
10.2.0.0/16 (VPC3)	-	-	-
10.3.0.0/16 (VPC4)	-	-	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$510 + \$12 (user) - \$255
VGW	\$72 - \$36
TGW	\$144 + data
Sum:	\$1146 + \$12/user + data

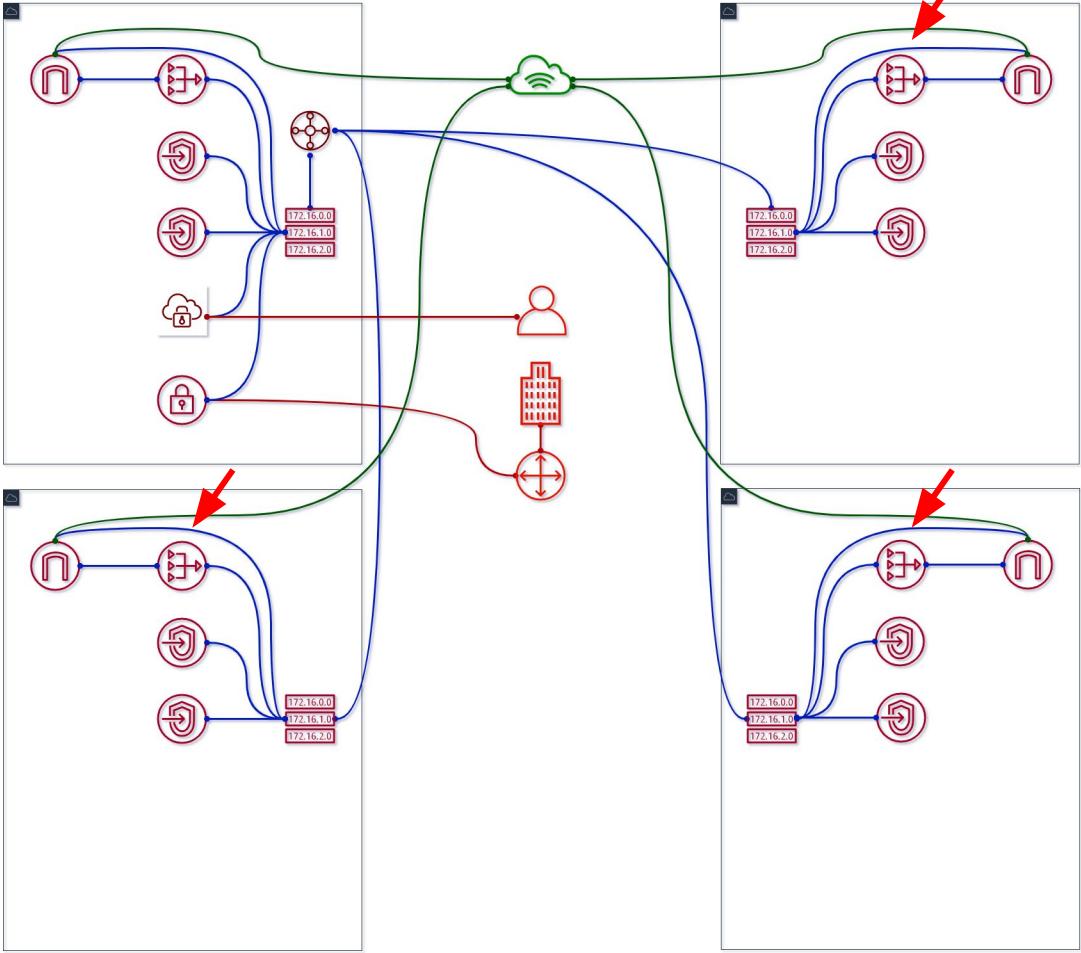


Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	
10.1.0.0/16 (VPC2)		igw-1...	-
10.2.0.0/16 (VPC3)		igw-2...	-
10.3.0.0/16 (VPC4)		igw-3...	-
0.0.0.0/0		igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1... tgw-2/3/4...	vgw-1... tgw-2/3/4...	subnet-1a/b/c
10.0.0.0/16 (VPC1)	-	-	-
10.1.0.0/16 (VPC2)	-	-	-
10.2.0.0/16 (VPC3)	-	-	-
10.3.0.0/16 (VPC4)	-	-	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-

Resources	Costs
NAT GW	\$420 + data
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
TGW	\$144 + data
Sum:	\$850 + \$12/user + data

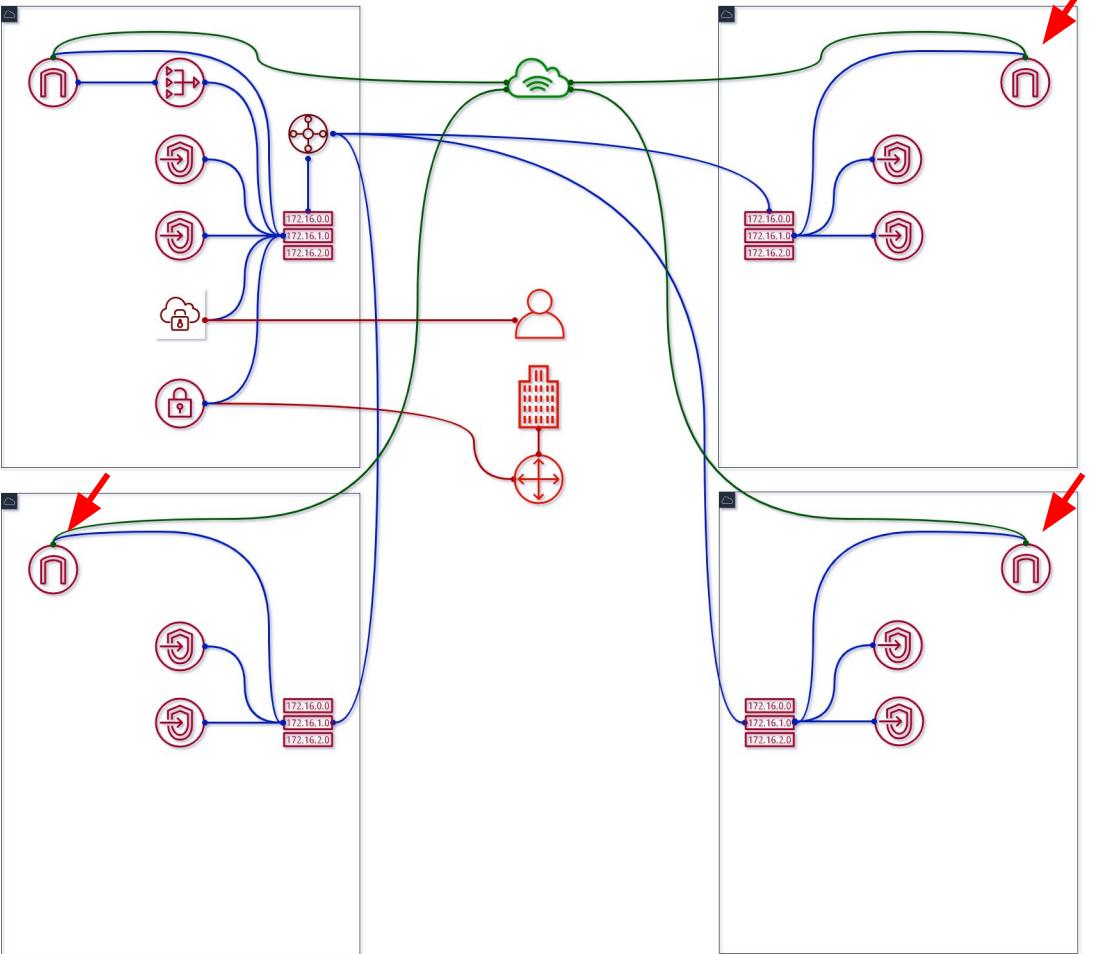
Can we improve it?

Now lower costs even further



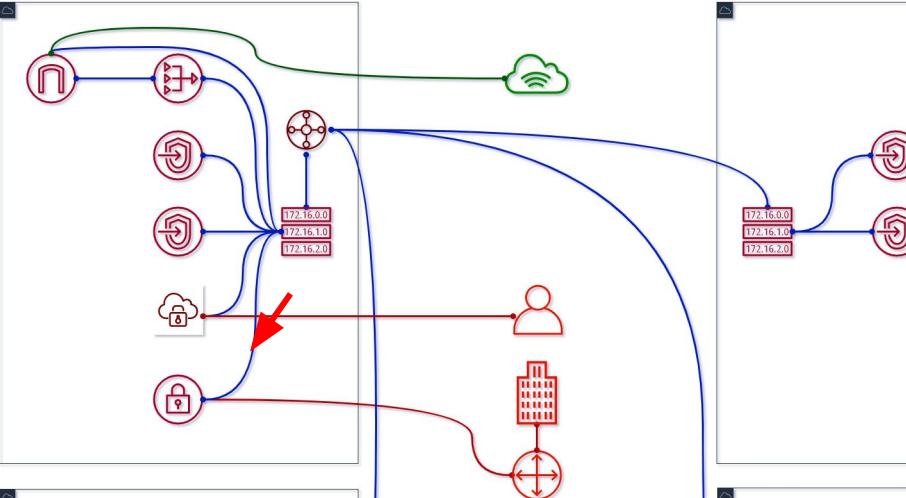
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)			
10.1.0.0/16 (VPC2)			
10.2.0.0/16 (VPC3)			
10.3.0.0/16 (VPC4)			
0.0.0.0/0	nat-1a/b/c... nat-2a/b/c... nat-3a/b/c... nat-4a/b/c...	igw-1... igw-2... igw-3... igw-4...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1... tgw-2/3/4...	vgw-1... tgw-2/3/4...	subnet-1a/b/c
10.0.0.0/16 (VPC1)	-	-	-
10.1.0.0/16 (VPC2)	-	-	-
10.2.0.0/16 (VPC3)	-	-	-
10.3.0.0/16 (VPC4)	-	-	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-

Resources	Costs
NAT GW	\$420 + data - \$315
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
TGW	\$144 + data
Sum:	\$850 + \$12/user + data

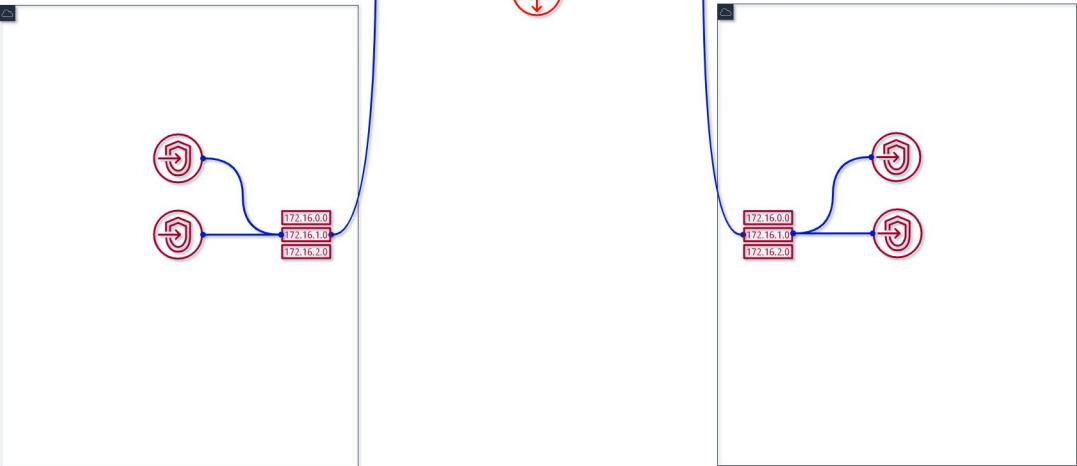


Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	
10.1.0.0/16 (VPC2)		igw-1... igw-2... igw-3... igw-4...	
10.2.0.0/16 (VPC3)			
10.3.0.0/16 (VPC4)			
0.0.0.0/0	nat-1a/b/c...		-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynamoDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1... tgw-2/3/4...	vgw-1... tgw-2/3/4...	subnet-1a/b/c
10.0.0.0/16 (VPC1)	-	-	-
10.1.0.0/16 (VPC2)	-	-	-
10.2.0.0/16 (VPC3)	-	-	-
10.3.0.0/16 (VPC4)	-	-	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-

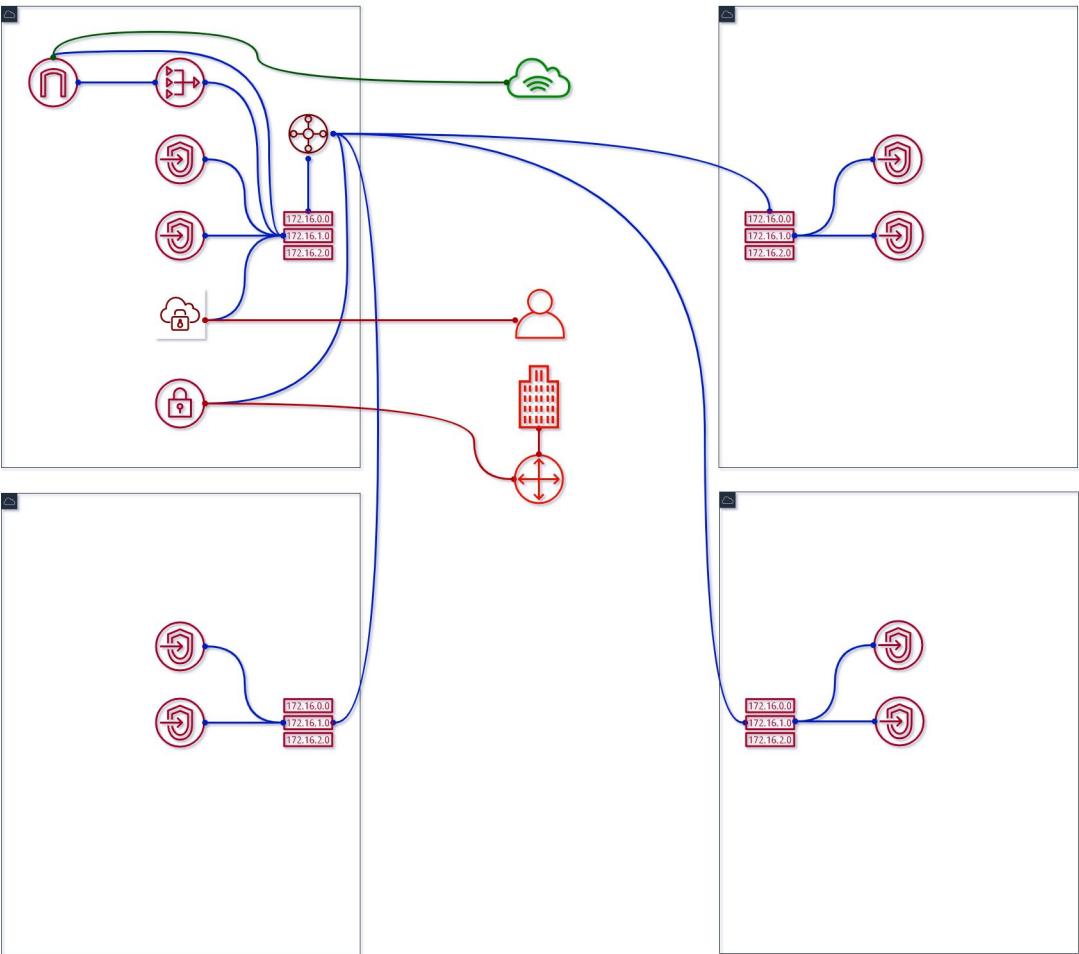
Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
TGW	\$144 + data
Sum:	\$540 + \$12/user + data



Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	
10.1.0.0/16 (VPC2)		igw-1...	
10.2.0.0/16 (VPC3)		-	
10.3.0.0/16 (VPC4)		-	
0.0.0.0/0	nat-1a/b/c...	igw-1...	-
pl... (S3)	vpc-1a/2a/3a/4a...	-	-
pl... (DynamoDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1... tgw-2/3/4...	vgw-1... tgw-2/3/4...	subnet-1a/b/c
10.0.0.0/16 (VPC1)	-	-	-
10.1.0.0/16 (VPC2)	-	-	-
10.2.0.0/16 (VPC3)	-	-	-
10.3.0.0/16 (VPC4)	-	-	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-



Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
TGW	\$144 + data
Sum:	\$540 + \$12/user + data

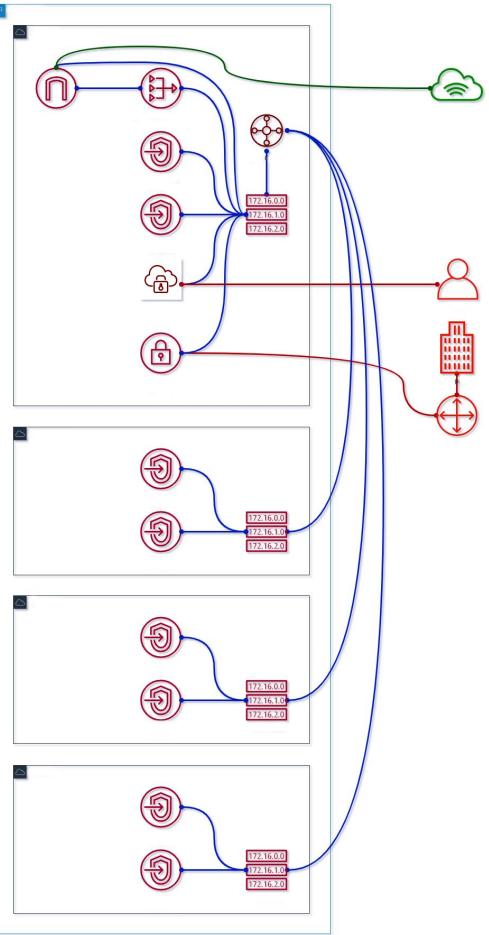


Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	
10.1.0.0/16 (VPC2)		igw-1...	
10.2.0.0/16 (VPC3)		-	
10.3.0.0/16 (VPC4)		-	
0.0.0.0/0	nat-1a/b/c...	igw-1...	-
pl-... (S3)	vpc-1a/2a/3a/4a...	-	-
pl-... (DynamoDB)	vpc-1b/2b/3b/4b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	tgw-1/2/3/4...	tgw-1/2/3/4...	subnet-1a/b/c
10.0.0.0/16 (VPC1)	-	-	-
10.1.0.0/16 (VPC2)	-	-	-
10.2.0.0/16 (VPC3)	-	-	-
10.3.0.0/16 (VPC4)	-	-	-
10.0.0.0/9 (Cloud)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-

Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
TGW	\$144 + \$36 + data
Sum:	\$576 + \$12/user + data

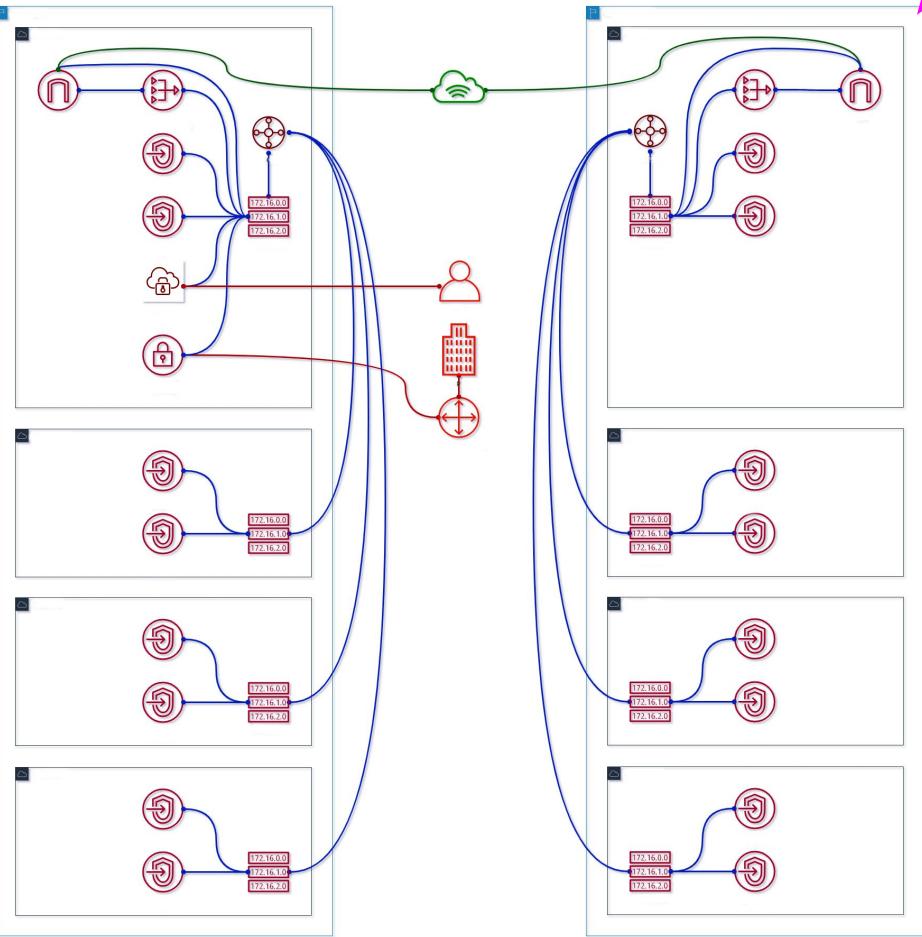
What is the limit?

And mirror everything in another region



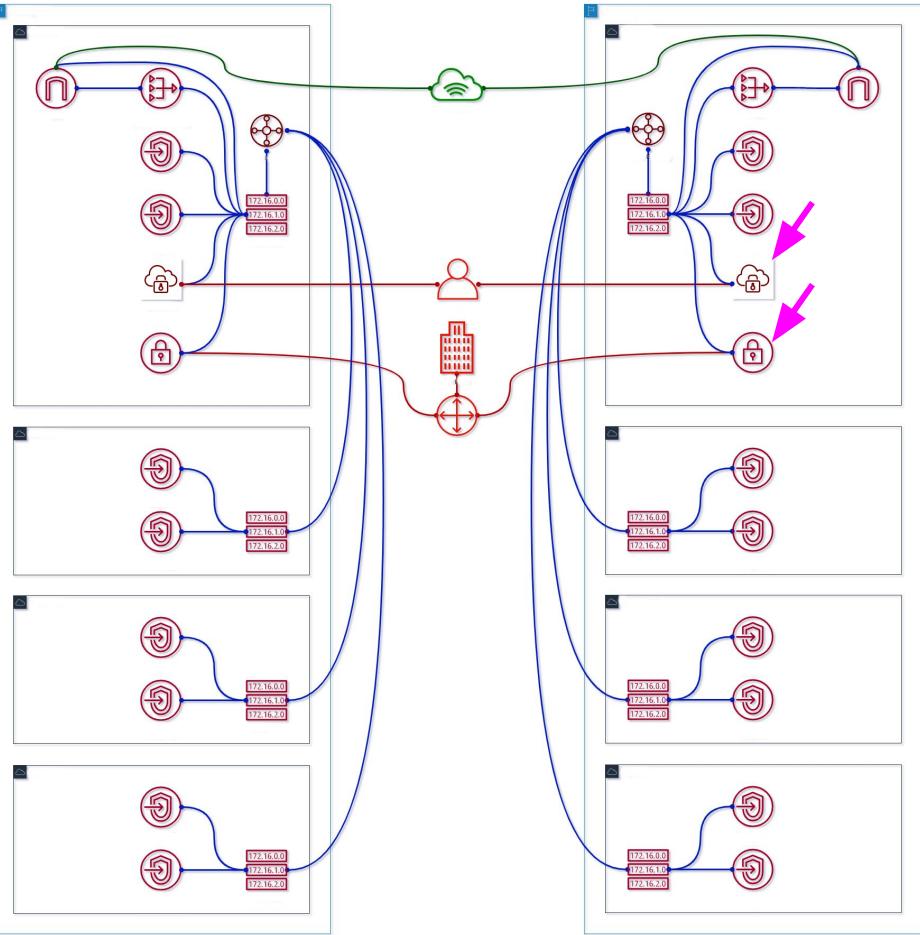
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)	Local	Local	subnet-1a/b/c
10.1.0.0/16 (VPC2)		igw-1...	-
10.2.0.0/16 (VPC3)		-	-
10.3.0.0/16 (VPC4)		vpc-1a/2a/3a/4a...	-
0.0.0.0/0	nat-1a/b/c...	vgw-1...	-
pl-... (S3)	vpc-1b/2b/3b/4b...	tgw-2/3/4...	-
pl-... (DynDB)			-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1... tgw-2/3/4...	vgw-1... tgw-2/3/4...	subnet-1a/b/c
10.0.0.0/13 (1st Region)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-
10.5.0.0/13 (2nd Region)	-	-	-

Resources	Costs
NAT GW	\$105 + data
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
TGW	\$180 + data
Sum:	\$576 + \$12/user + data



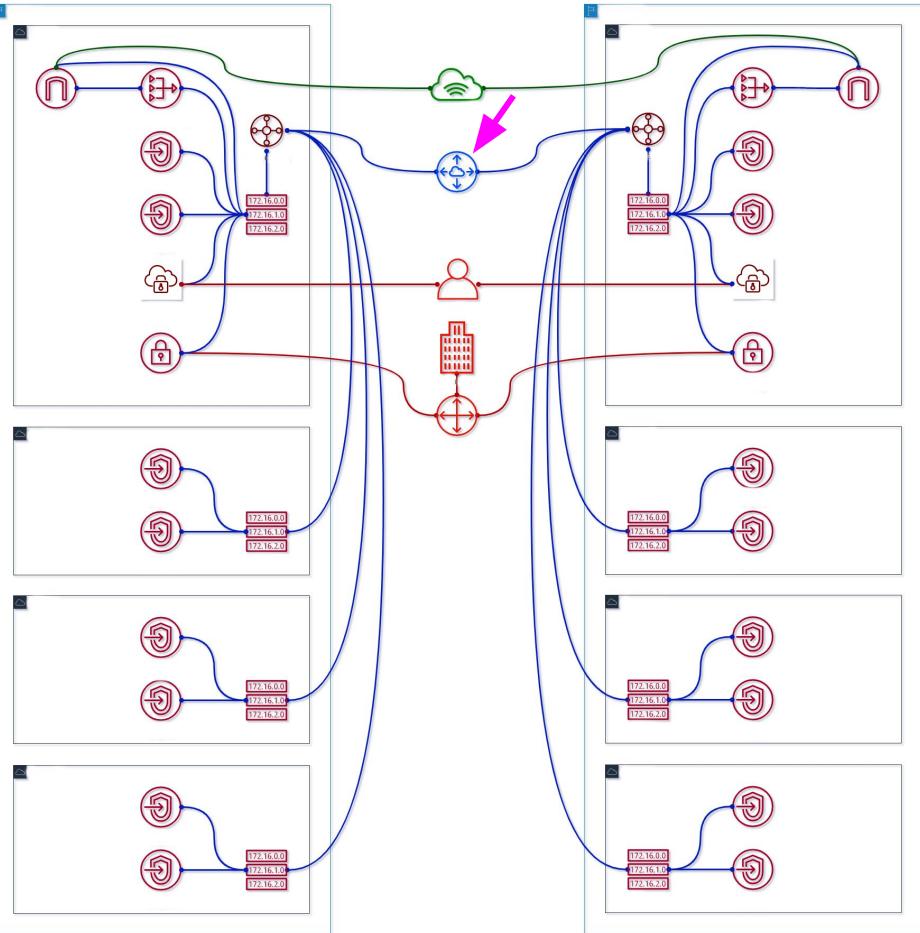
Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)			
10.1.0.0/16 (VPC2)			
10.2.0.0/16 (VPC3)			
10.3.0.0/16 (VPC4)			
10.4.0.0/16(VPC5)	Local	Local	subnet-1a/b/c
10.5.0.0/16(VPC6)			
10.6.0.0/16(VPC7)			
10.7.0.0/16(VPC8)			
0.0.0.0/0	nat-1a/b/c... nat-5a/b/c...	igw-1... igw-5...	-
pl... (S3)	vpc-1a/2a/3a/4a /5a/6a/7a/8a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b /5b/6b/7b/8b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c
10.128.0.0/9 (Corp)	vgw-1... tgw-2/3/4...	vgw-1... tgw-2/3/4...	subnet-1a/b/c
10.0.0.0/13 (1st Region)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-
10.5.0.0/13 (2nd Region)	tgw-att-5/6/7/8...	tgw-att-5/6/7/8...	-

Resources	Costs
NAT GW	\$105 + data + \$105
IGW	data
VPE	\$255 + \$12 (user)
VGW	\$36
TGW	\$180 + data + \$144
Sum:	\$861 + \$12/user + data



Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)			
10.1.0.0/16 (VPC2)			
10.2.0.0/16 (VPC3)			
10.3.0.0/16 (VPC4)			
10.4.0.0/16(VPC5)			
10.5.0.0/16(VPC6)			
10.6.0.0/16(VPC7)			
10.7.0.0/16(VPC8)			
0.0.0.0/0	nat-1a/b/c... nat-5a/b/c...	igw-1... igw-5...	-
pl... (S3)	vpc-1a/2a/3a/4a /5a/6a/7a/8a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b /5b/6b/7b/8b...	-	-
169.254.169.252 /30 (AWS)	-		subnet-1a/b/c subnet-5a/b/c
10.128.0.0/9 (Corp)	vgw-1/5... tgw-2/3/4/6/7/8...	vgw-1/5... tgw-2/3/4/6/7/8...	subnet-1a/b/c subnet-5a/b/c
10.0.0.0/13 (1st Region)	tgw-att-1/2/3/4...	tgw-att-1/2/3/4...	-
10.5.0.0/13 (2nd Region)	tgw-att-5/6/7/8...	tgw-att-5/6/7/8...	-

Resources	Costs
NAT GW	\$210 + data
IGW	data
VPE	\$510 + \$12 (user)
VGW	\$72
TGW	\$324 + data
Sum:	\$1116 + \$12/user + data



Destination	Private	Public	VPE
10.0.0.0/16 (VPC1)			
10.1.0.0/16 (VPC2)			
10.2.0.0/16 (VPC3)			
10.3.0.0/16 (VPC4)			
10.4.0.0/16(VPC5)			
10.5.0.0/16(VPC6)			
10.6.0.0/16(VPC7)			
10.7.0.0/16(VPC8)			
0.0.0.0/0	nat-1a/b/c... nat-5a/b/c...	igw-1... igw-5...	-
pl... (S3)	vpc-1a/2a/3a/4a /5a/6a/7a/8a...	-	-
pl... (DynDB)	vpc-1b/2b/3b/4b /5b/6b/7b/8b...	-	-
169.254.169.252 /30 (AWS)	-	-	subnet-1a/b/c subnet-5a/b/c
10.128.0.0/9 (Corp)	vgw-1/5... tgw-2/3/4/6/7/8...	vgw-1/5... tgw-2/3/4/6/7/8...	subnet-1a/b/c subnet-5a/b/c
10.0.0.0/13 (1st Region)	tgw-att-1/2/3/4... pcx-5...	tgw-att-1/2/3/4... pcx-5...	-
10.5.0.0/13 (2nd Region)	tgw-att-5/6/7/8... pcx-1...	tgw-att-5/6/7/8... pcx-1...	-

Resources	Costs
NAT GW	\$210 + data
IGW	data
VPE	\$510 + \$12 (user)
VGW	\$72
TGW	\$423 + data
Sum:	\$1116 + \$12/user + data

SUMMARY COMPARISON

Accounts	Peering	Transit Gateway	Transit Gateway + Egress
1	\$396	\$432	\$432
2	\$792 (+396)	\$573 (+141)	\$468 (+36)
3	\$1'188 (+396)	\$714 (+141)	\$504 (+36)
4	\$1'584 (+396)	\$855 (+141)	\$540 (+36)
9	\$3'564 (+1980)	\$1'560 (+705)	\$720 (+180)
15	\$5'940 (+2376)	\$2'406 (+846)	\$936 (+216)
100	-	\$14'391 (+11985)	\$3'996 (+3060)

CONNECTING COUPLE OF VPCS

VPC PEERING

- Up to 9 VPCs or 15 if requested limit increase on peering (50-125)

CONNECTING MANY VPCS

TRANSIT GATEWAY

- Up to 5000 attachments
- 20 route tables (routing domain) per Transit Gateway

CONNECTING MULTIPLE REGIONS AND MANY VPCS

VPC PEERING

+

TRANSIT GATEWAY



THANK YOU

Krysztof Szyper

Managing networking chaos while migrating to AWS multi-account architecture