Ralph Klos
PROJECTS & CONSULTANCY

GUIDE

Working with the VPC Builder

A VPC with subnets, routes, NACLs and endpoints, as Terraform and CloudFormation

FOR
Cloud, network and platform teams

FROM
Ralph Klos Projects & Consultancy

VERSION
VPC Builder 0.1

DATE
6 October 2026

Contents

1. In short 3

2. Opening it 3

3. Working with the builder 4

4. Reading the result 6

5. Reviewing an existing VPC 6

6. Deploying 7

7. Projects and later changes 8

8. Safety, limits and liability 8

1. In short

The VPC Builder designs a complete VPC: a public tier, an application tier and a data tier across at least two Availability Zones, with the routes, NAT, endpoints, flow logs and the NACLs that fit your risk. You see the diagram, the IP plan, the routes, the NACL rules, advice and the fixed cost straight away, and you get the design as Terraform and as CloudFormation.

- **Free, with an account:** the builder is in the customer portal on rkpc.be. You create a free account with your name, company and email address, protected with a password and an authenticator app.
- **Everything in your browser:** the page does not call AWS, asks for no keys and sends your design nowhere. The page fixes that itself in its Content-Security-Policy.
- **You deploy it yourself:** the builder makes the files; you read them, test them and deploy them.
- **Dutch and English:** switch with **NL / EN** at the top. Your choices stay stored in the browser.

> A network decides what the internet can reach in your account. A wrong setting, or a file you deploy without reading it, can open your account. Only use the builder if you know VPCs, route tables, NACLs and security groups, or have the result reviewed by someone who does.

2. Opening it

	STEP
1	Go to **rkpc.be/portal** and sign in. No account yet? Click **Create an account**; you get an email with a link to set your password and authenticator app.
2	In the portal, click **Open** at **VPC Builder**.
3	The first time, the page asks for a confirmation (see below). Tick both boxes and click **Agree, open the VPC Builder**.
4	The builder opens. The browser remembers the last state; **New** clears everything, after a confirmation.

2.1 The confirmation first

Before the first use you confirm this:

- A wrong setting, or a file you deploy without reading it, can open your AWS account to the internet.
- You know VPCs, subnets, route tables, NACLs and security groups, or someone who does reviews the result.
- You read every file, check `terraform plan` or the change set, and test in an account without production first.
- You are responsible for what you deploy, and for the AWS costs.
- The tool is free and provided as is, without warranty. To the extent the law allows, RKPC (Ralph Klos Projects & Consultancy) is not liable for damage, data leaks, outages or costs from its use.

Your agreement is kept with your account, with the date, the version of the text and the IP address. When the text changes, the page asks again.

3. Working with the builder

The choices are on the left, from top to bottom; the result is on the right and updates with every change. At the top of the result you see the number of subnets, the number of NACL rules and the fixed cost per month.

1. Account → 2. VPC → 3. Tiers → 4. Internet → 5. NACLs → 6. Logging

3.1 What kind of account is it?

OPTION	WHAT THE BUILDER MAKES
A normal AWS account	The VPC goes to the internet itself, with an internet gateway and NAT. A Transit Gateway can be added.
Connected to the internal network	The account hangs on the company network through a Transit Gateway (landing zone). The IP block comes from the network team.
Central egress	For a connected account: the default route of the private tiers goes to the Transit Gateway, without NAT of its own and without a public tier.
Networks behind the Transit Gateway	CIDRs of other VPCs and on-premises, e.g. `10.0.0.0/8`. They get a route and may come in through the NACLs.
Share through AWS RAM	For a network account: other accounts put their servers in your subnets, but do not manage the routes and NACLs. You pick with whom and which tiers.

3.2 The VPC

- **Name prefix:** the start of every name, e.g. `prod` gives `prod-app-1`.
- **Region and IP block:** a CIDR between /16 and /28. The subnets move along when you change the size.
- **Availability Zones:** 2, 3 or 4. At least two: every tier gets a subnet per AZ, so it keeps working when an AZ fails.
- **IPv6:** dual-stack, with a /56 from Amazon.
- **More regions:** the same design in another region, each with its own IP block that does not overlap. The region goes into the names (`main-euw1-app-1`). A region can get tiers of its own, e.g. a smaller disaster-recovery region without a data tier.

3.3 Tiers (subnets)

TIER	WHAT BELONGS IN IT
Public	Load balancers and NAT gateways. This is where the internet comes in; servers do not belong here.
Application	Servers, containers and Lambdas in a VPC. No public IP; out through NAT.
Data	Databases, caches and file storage with the company data; no applications. Only the application tier reaches it, and the tier never has internet: S3 and DynamoDB through the gateway endpoints.
Transit	Small subnets (/28) for the Transit Gateway attachment.

Every tier gets one subnet per AZ, with the size you pick. A /16 gets a public /24, an application /20 and a data /22 by default.

3.4 Internet and endpoints

OPTION	EFFECT
No NAT	The application tier cannot reach the internet; only through endpoints.
One NAT gateway	Cheaper, but fails with its AZ.
One NAT gateway per AZ	Recommended for production.
Gateway endpoints	S3 and DynamoDB, free. The traffic stays on the AWS network.
Interface endpoints	Session Manager, ECR, CloudWatch Logs, STS, KMS, Secrets Manager, SQS and SNS, without NAT. Paid per endpoint, per AZ, per hour.
Endpoint policy (organization ID)	With e.g. `o-exampleorg1` the endpoints only let your own accounts through, and AWS services on your behalf. The Session Manager channels and S3 stay open (see the advice).

3.5 NACL level

NACLs work per subnet and do not remember connections; they are the second line of defence next to the security groups. The stricter, the more you need to know about what runs.

LEVEL	WHAT IT DOES
Off	The AWS default NACL: everything is allowed. The security groups do all the work.
Basic	Known dangerous ports closed from the internet, and tiers cannot skip each other: public never reaches data directly.
Strict	Only the ports of the chosen services, plus the return traffic (ephemeral ports).
Locked down	Strict, plus: SSH and RDP explicitly denied, no HTTP outbound, the default NACL closed and flow logs of rejected traffic.

For Strict and Locked down you fill in the ports: what is open from the internet (public tier), the ports of the application (from the load balancer), the databases and caches in the data tier, and optionally admin from a fixed IP.

> Rather no admin port: Session Manager needs no open port. Turn on the Session Manager endpoint and the servers are reachable without SSH or RDP.

3.6 Logging and defaults

- **VPC flow logs:** to CloudWatch Logs (with a retention) or an S3 bucket; everything or only rejected traffic. With more accounts AWS recommends a central bucket in the log archive account.
- **Encryption of the logs:** the AWS key, a new KMS key per region (about € 1 per month), or an existing key.
- **Empty the default security group:** the CIS recommendation.
- **VPC Block Public Access:** for the whole account in that region. Block inbound with the public subnets excluded, or block in and out (without public tier and IPv6). It also applies to VPCs made by hand later.
- **Tags:** key and optional value; they go on every resource of the VPC.

> Block Public Access applies to the whole account in the region, not only to this VPC. First check whether there are other VPCs with internet traffic: they are blocked too, unless you exclude them.

4. Reading the result

VIEW	WHAT YOU SEE
Diagram	The VPC with the AZs, the tiers, the gateways and the endpoints. Click to enlarge: zoom in and out and pan inside the page. **Download diagram** gives an SVG.
IP plan	Every subnet with its name, AZ, CIDR and number of addresses, and what is still free in the VPC.
Routes	The route tables per tier: destination and through (local, internet gateway, NAT, Transit Gateway, endpoint).
NACLs	Every rule per tier, in and out, with its number, port, from or to, and why it is there.
Advice	Remarks on this design, the fixed cost per part and the source of the prices.
Files	`<prefix>-vpc.tf` (Terraform) and `<prefix>-vpc.yaml` (CloudFormation), to copy or download. With more regions one set per region.

The costs are AWS list prices for eu-west-1 (Ireland), without data traffic: NAT gateways, public IPv4 addresses, interface endpoints, Transit Gateway attachments and KMS keys. Subnets, route tables, NACLs and gateway endpoints are free. AWS gives the prices in dollars; the VPC Builder shows them in euro, converted at the ECB reference rate (the date and the rate are under the cost table). Prices and the rate change: the links in the advice show the current price.

5. Reviewing an existing VPC

Under **Review an existing VPC** the builder compares a VPC that already exists with the best practices: open NACLs, the default security group, flow logs, NAT and endpoints.

	STEP
1	Download the script for bash or PowerShell and run it in a terminal where the AWS CLI is signed in. It only reads (`describe-*`), needs no more than ReadOnlyAccess and writes one JSON file.
2	Click **Open export...** and pick the file. It is read in your browser and sent nowhere.
3	Pick the VPC and read the findings (high, medium, low, in order). **Use as the starting point of the design** takes over the IP block, AZs, IPv6, NAT, endpoints and flow logs.

```
bash rkpc-vpc-export.sh eu-west-1
# or in PowerShell:
powershell -ExecutionPolicy Bypass -File rkpc-vpc-export.ps1 -Region eu-west-1
```

> Read the script before you run it: it is short and holds only `aws ec2 describe-*` calls. The export holds the IDs, IP blocks and tags of that region: treat it like internal documentation.

6. Deploying

Always deploy to an account without production first. Check what AWS will do before you apply anything, and only then move on to test and production.

6.1 With Terraform

Put the `.tf` file in a folder of its own (its own state per region) and run:

```
terraform init
terraform plan -out vpc.plan
terraform apply vpc.plan
```

6.2 With CloudFormation

Create a change set first and review it, in the console or like this:

```
aws cloudformation create-change-set --stack-name main-vpc \
  --template-body file://main-vpc.yaml --change-set-type CREATE --change-set-name first
aws cloudformation describe-change-set --stack-name main-vpc --change-set-name first
aws cloudformation execute-change-set --stack-name main-vpc --change-set-name first
```

CloudFormation cannot empty the default security group and the default NACL. If you chose that, the top of the template holds the AWS CLI commands to run after the stack.

6.3 Testing

- **What must work:** the load balancer from the internet, the application to the database, Session Manager to the servers, and updates through NAT or endpoints.
- **What must be denied:** the data tier to the internet, the public tier straight to the data tier, and the ports you did not open.
- **Flow logs:** look for `REJECT` on traffic you did expect. That shows which NACL rule is missing.

> A NACL also denies the return traffic if the ephemeral ports are not open, and it allows at most 20 rules per direction. Change rules in the builder rather than by hand, so the design and reality stay the same.

7. Projects and later changes

Name the project and click **Save**. You get a readable JSON file with every choice. Put it in Git next to the Terraform or the template.

- A change needed? Click **Open...** and pick the file: every choice is back as it was saved.
- Make the files again and have the difference reviewed (`git diff`, `terraform plan`) before you deploy.
- A file that does not come from the builder is refused; unknown values are ignored.

> The project file holds IP blocks, account IDs and the IDs of your organization and Transit Gateway. Keep it where the network code is, not in a public repository.

8. Safety, limits and liability

- **No AWS access:** the builder asks for no keys, calls no AWS API and sends nothing out. The portal only records that you opened the tool.
- **Public sources:** the design follows the AWS documentation on VPCs, NACLs and endpoints, and the CIS recommendations.
- **A starting point, not a guarantee:** every network is different. Read every file and test in an account without production first.
- **Security groups** are not made by the builder: they belong to the application. The NACLs are the second line.
- **Prices** are an estimate based on list prices, without data traffic.

> The VPC Builder is free and provided as is, without warranty. You are responsible for what you deploy and for the AWS costs. To the extent the law allows, RKPC (Ralph Klos Projects & Consultancy) is not liable for damage, data leaks, outages or costs from its use.

Your free account stays until you ask to delete it, or until 2 years without signing in; after that it is deleted automatically. Help with the design or the rollout? Email ralph@rkpc.be or visit rkpc.be.