Ralph Klos
PROJECTS & CONSULTANCY

HANDLEIDING

Werken met de VPC Builder

Een VPC met subnets, routes, NACL's en endpoints, als Terraform en CloudFormation

VOOR
Cloud-, netwerk- en platformteams

VAN
Ralph Klos Projects & Consultancy

VERSIE
VPC Builder 0.1

DATUM
6 oktober 2026

Inhoud

1. In het kort 3

2. Openen 3

3. Werken met de builder 4

4. Het resultaat lezen 6

5. Een bestaande VPC nakijken 6

6. Uitrollen 7

7. Projecten en latere wijzigingen 8

8. Veiligheid, grenzen en aansprakelijkheid 8

1. In het kort

De VPC Builder ontwerpt een volledige VPC: een publieke laag, een applicatielaag en een datalaag over minstens twee beschikbaarheidszones, met de routes, NAT, endpoints, flow logs en de NACL's die bij uw risico passen. U ziet meteen het schema, het IP-plan, de routes, de NACL-regels, advies en de vaste kosten, en u krijgt het ontwerp als Terraform en als CloudFormation.

- **Gratis, met een account:** de builder staat in het klantenportaal op rkpc.be. U maakt gratis een account met uw naam, bedrijf en e-mailadres, beveiligd met een wachtwoord en een authenticator-app.
- **Alles in uw browser:** de pagina roept AWS niet aan, vraagt geen sleutels en stuurt uw ontwerp nergens naartoe. Dat legt de pagina zelf vast in haar Content-Security-Policy.
- **U rolt zelf uit:** de builder maakt de bestanden; u leest ze na, test ze en rolt ze uit.
- **Nederlands en Engels:** wissel met **NL / EN** bovenaan. Uw keuzes blijven in de browser bewaard.

> Een netwerk bepaalt wat het internet in uw account kan bereiken. Een verkeerde instelling, of een bestand dat u uitrolt zonder het na te lezen, kan uw account openzetten. Gebruik de builder alleen als u VPC's, route tables, NACL's en security groups kent, of laat het resultaat nalezen door iemand die dat doet.

2. Openen

	STAP
1	Ga naar **rkpc.be/portal** en meld u aan. Nog geen account? Klik **Account aanmaken**; u krijgt een e-mail met een link om uw wachtwoord en authenticator-app in te stellen.
2	Klik op het portaal bij **VPC Builder** op **Openen**.
3	De eerste keer vraagt de pagina een bevestiging (zie hieronder). Vink beide vakjes aan en klik **Akkoord, open de VPC Builder**.
4	De builder opent. De browser onthoudt de laatste stand; **Nieuw** maakt alles leeg, na een bevestiging.

2.1 De bevestiging vooraf

Voor het eerste gebruik bevestigt u dit:

- Een verkeerde instelling, of een bestand dat u uitrolt zonder het na te lezen, kan uw AWS-account openzetten naar het internet.
- U kent VPC's, subnetten, route tables, NACL's en security groups, of iemand die dat kent leest het resultaat na.
- U leest elk bestand na, bekijkt `terraform plan` of de change set, en test eerst in een account zonder productie.
- U bent zelf verantwoordelijk voor wat u uitrolt, en voor de kosten bij AWS.
- De tool is gratis en wordt gegeven zoals hij is, zonder garantie. Voor zover de wet dat toelaat, is RKPC (Ralph Klos Projects & Consultancy) niet aansprakelijk voor schade, datalekken, onderbrekingen of kosten door het gebruik ervan.

Uw akkoord wordt bij uw account bewaard, met de datum, de versie van de tekst en het IP-adres. Verandert de tekst, dan vraagt de pagina het opnieuw.

3. Werken met de builder

Links staan de keuzes, van boven naar beneden; rechts het resultaat, dat bij elke wijziging meteen bijwerkt. Bovenaan het resultaat ziet u het aantal subnets, het aantal NACL-regels en de vaste kosten per maand.

1 1. Account → 2 2. VPC → 3 3. Lagen → 4 4. Internet → 5 5. NACL's → 6 6. Logging

3.1 Wat voor account is het?

KEUZE	WAT DE BUILDER MAAKT
Een gewoon AWS-account	De VPC gaat zelf naar het internet, met een internet gateway en NAT. Een Transit Gateway kan erbij.
Verbonden met het interne netwerk	Het account hangt via een Transit Gateway aan het bedrijfsnetwerk (landing zone). Het IP-blok komt van het netwerkteam.
Centrale uitgang	Bij een verbonden account: de standaardroute van de private lagen gaat naar de Transit Gateway, zonder eigen NAT en zonder publieke laag.
Netwerken achter de Transit Gateway	CIDR's van andere VPC's en on-premises, bv. `10.0.0.0/8`. Ze krijgen een route en mogen binnen in de NACL's.
Delen via AWS RAM	Voor een netwerkaccount: andere accounts zetten hun servers in uw subnets, maar beheren de routes en NACL's niet. U kiest met wie en welke lagen.

3.2 De VPC

- **Naamprefix:** het begin van elke naam, bv. `prod` geeft `prod-app-1`.
- **Regio en IP-blok:** een CIDR tussen /16 en /28. De subnets schuiven mee als u de grootte wijzigt.
- **Beschikbaarheidszones:** 2, 3 of 4. Minstens twee: elke laag krijgt een subnet per AZ, zodat ze blijft werken als een AZ uitvalt.
- **IPv6:** dual-stack, met een /56 van Amazon.
- **Meer regio's:** hetzelfde ontwerp in een andere regio, elk met een eigen IP-blok dat niet overlapt. De regio komt in de namen (`main-euw1-app-1`). Een regio kan eigen lagen krijgen, bv. een kleinere regio voor noodherstel zonder datalaag.

3.3 Lagen (subnets)

LAAG	WAT ERIN HOORT
Publiek	Load balancers en NAT-gateways. Hier komt het internet binnen; servers horen hier niet.
Applicatie	Servers, containers en Lambda's in een VPC. Geen publiek IP; naar buiten via NAT.
Data	Databases, caches en bestandsopslag met de bedrijfsdata; geen applicaties. Alleen de applicatielaag bereikt haar, en de laag heeft nooit internet: S3 en DynamoDB via de gateway-endpoints.
Transit	Kleine subnets (/28) voor de koppeling met een Transit Gateway.

Elke laag krijgt één subnet per AZ, met de grootte die u kiest. Een /16 krijgt standaard een publieke /24, een applicatie-/20 en een data-/22.

3.4 Internet en endpoints

KEUZE	EFFECT
Geen NAT	De applicatielaag kan niet naar het internet; alleen via endpoints.
Eén NAT-gateway	Goedkoper, maar valt uit met zijn AZ.
Eén NAT-gateway per AZ	Aanbevolen voor productie.
Gateway-endpoints	S3 en DynamoDB, gratis. Het verkeer blijft op het AWS-netwerk.
Interface-endpoints	Session Manager, ECR, CloudWatch Logs, STS, KMS, Secrets Manager, SQS en SNS, zonder NAT. Betalend per endpoint, per AZ, per uur.
Endpoint-policy (organisatie-ID)	Met bv. `o-exampleorg1` laten de endpoints alleen uw eigen accounts door, en AWS-diensten namens u. De kanalen van Session Manager en S3 blijven open (zie het advies).

3.5 NACL-niveau

NACL's werken per subnet en onthouden geen verbindingen; ze zijn de tweede verdedigingslijn naast de security groups. Hoe strenger, hoe meer u moet weten over wat er draait.

NIVEAU	WAT HET DOET
Uit	De standaard-NACL van AWS: alles mag. De security groups doen al het werk.
Basis	Bekende gevaarlijke poorten dicht vanaf het internet, en lagen kunnen elkaar niet overslaan: publiek komt nooit rechtstreeks bij data.
Strikt	Alleen de poorten van de gekozen diensten, plus het terugverkeer (ephemeral poorten).
Afgesloten	Strikt, plus: SSH en RDP expliciet dicht, geen HTTP naar buiten, de standaard-NACL dicht en flow logs van geweigerd verkeer.

Bij Strikt en Afgesloten vult u de poorten in: wat open staat vanaf het internet (publieke laag), de poorten van de applicatie (vanaf de load balancer), de databases en caches in de datalaag, en eventueel beheer vanaf een vast IP.

> Liever geen beheerpoort: Session Manager heeft geen open poort nodig. Zet het Session Manager-endpoint aan en de servers zijn bereikbaar zonder SSH of RDP.

3.6 Logging en standaardinstellingen

- **VPC flow logs:** naar CloudWatch Logs (met bewaartermijn) of een S3-bucket; alles of alleen geweigerd verkeer. Met meer accounts raadt AWS een centrale bucket in het log-archiefaccount aan.
- **Versleuteling van de logs:** de sleutel van AWS, een nieuwe KMS-sleutel per regio (± € 1 per maand), of een bestaande sleutel.
- **De standaard security group leegmaken:** de CIS-aanbeveling.
- **VPC Block Public Access:** voor de hele account in die regio. Inkomend blokkeren met de publieke subnets uitgezonderd, of in en uit blokkeren (zonder publieke laag en IPv6). Het geldt ook voor VPC's die later met de hand gemaakt worden.
- **Tags:** sleutel en optionele waarde; ze komen op elke resource van de VPC.

> Block Public Access geldt voor het hele account in de regio, niet alleen voor deze VPC. Kijk eerst na of er andere VPC's met internetverkeer zijn: die worden mee geblokkeerd, tenzij u ze uitzondert.

4. Het resultaat lezen

WEERGAVE	WAT U ZIET
Schema	De VPC met de AZ's, de lagen, de gateways en de endpoints. Klik om te vergroten: in- en uitzoomen en verschuiven binnen de pagina. **Schema downloaden** geeft een SVG.
IP-plan	Elk subnet met zijn naam, AZ, CIDR en aantal adressen, en wat nog vrij is in de VPC.
Routes	De route tables per laag: bestemming en via (lokaal, internet gateway, NAT, Transit Gateway, endpoint).
NACL's	Elke regel per laag, in en uit, met het nummer, de poort, van of naar, en waarom ze er staat.
Advies	Opmerkingen bij dit ontwerp, de vaste kosten per onderdeel en de bron van de prijzen.
Bestanden	`<prefix>-vpc.tf` (Terraform) en `<prefix>-vpc.yaml` (CloudFormation), om te kopiëren of te downloaden. Bij meer regio's één set per regio.

De kosten zijn lijstprijzen van AWS voor eu-west-1 (Ierland), zonder dataverkeer: NAT-gateways, publieke IPv4-adressen, interface-endpoints, Transit Gateway-koppelingen en KMS-sleutels. Subnets, route tables, NACL's en gateway-endpoints zijn gratis. AWS geeft de prijzen in dollar; de VPC Builder toont ze in euro, omgerekend tegen de referentiekoers van de ECB (de datum en de koers staan onder de kostentabel). Prijzen en koers veranderen: de links in het advies tonen de actuele prijs.

5. Een bestaande VPC nakijken

Onder **Een bestaande VPC nakijken** vergelijkt de builder een VPC die al bestaat met de best practices: open NACL's, de standaard security group, flow logs, NAT en endpoints.

	STAP
1	Download het script voor bash of PowerShell en draai het in een terminal waar de AWS CLI aangemeld is. Het leest alleen (`describe-*`), heeft genoeg aan ReadOnlyAccess en schrijft één JSON-bestand.
2	Klik **Export openen…** en kies het bestand. Het wordt in uw browser gelezen en nergens naartoe gestuurd.
3	Kies de VPC en lees de bevindingen (hoog, middel, laag, in orde). Met **Als vertrekpunt in het ontwerp zetten** neemt de builder het IP-blok, de AZ's, IPv6, NAT, endpoints en flow logs over.

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

> Lees het script voor u het draait: het is kort en bevat alleen `aws ec2 describe-*`-oproepen. De export bevat de ID's, IP-blokken en tags van die regio: behandel ze als interne documentatie.

6. Uitrollen

Rol altijd eerst uit in een account zonder productie. Kijk na wat AWS zal doen voor u iets toepast, en ga pas daarna naar test en productie.

6.1 Met Terraform

Zet het `.tf`-bestand in een eigen map (eigen state per regio) en draai:

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

6.2 Met CloudFormation

Maak eerst een change set en bekijk die, in de console of zo:

```
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 kan de standaard security group en de standaard-NACL niet leegmaken. Koos u dat, dan staan bovenaan de template de AWS CLI-commando's om na de stack te draaien.

6.3 Testen

- **Wat moet werken:** de load balancer vanaf het internet, de applicatie naar de database, Session Manager naar de servers, en de updates via NAT of endpoints.
- **Wat geweigerd moet worden:** de datalaag naar het internet, de publieke laag rechtstreeks naar de datalaag, en de poorten die u niet opende.
- **Flow logs:** zoek naar `REJECT` voor verkeer dat u wel verwacht. Zo ziet u welke NACL-regel ontbreekt.

> Een NACL weigert ook het terugverkeer als de ephemeral poorten niet open staan, en ze laat maximaal 20 regels per richting toe. Wijzig regels liefst in de builder, niet met de hand, zodat het ontwerp en de werkelijkheid gelijk blijven.

7. Projecten en latere wijzigingen

Geef het project een naam en klik **Bewaren**. U krijgt een leesbaar JSON-bestand met elke keuze. Zet het in Git naast de Terraform of de template.

- Een wijziging nodig? Klik **Openen…** en kies het bestand: alle keuzes staan weer zoals bij het bewaren.
- Maak de bestanden opnieuw en laat het verschil reviewen (`git diff`, `terraform plan`) voor u uitrolt.
- Een bestand dat niet van de builder komt, wordt geweigerd; onbekende waarden worden genegeerd.

> Het projectbestand bevat IP-blokken, account-ID's en de ID's van uw organisatie en Transit Gateway. Bewaar het waar de netwerkcode staat, niet in een publieke repository.

8. Veiligheid, grenzen en aansprakelijkheid

- **Geen AWS-toegang:** de builder vraagt geen sleutels, roept geen AWS-API aan en stuurt niets weg. Het portaal registreert alleen dat u de tool opende.
- **Openbare bronnen:** het ontwerp volgt de AWS-documentatie over VPC's, NACL's en endpoints, en de CIS-aanbevelingen.
- **Een startpunt, geen garantie:** elk netwerk is anders. Lees elk bestand na en test eerst in een account zonder productie.
- **Security groups** maakt de builder niet: die horen bij de applicatie. De NACL's zijn de tweede lijn.
- **Prijzen** zijn een schatting op basis van lijstprijzen, zonder dataverkeer.

> De VPC Builder is gratis en wordt gegeven zoals hij is, zonder garantie. U bent zelf verantwoordelijk voor wat u uitrolt en voor de kosten bij AWS. Voor zover de wet dat toelaat, is RKPC (Ralph Klos Projects & Consultancy) niet aansprakelijk voor schade, datalekken, onderbrekingen of kosten door het gebruik ervan.

Uw gratis account blijft bestaan tot u vraagt het te verwijderen, of tot 2 jaar zonder aanmelding; daarna wordt het automatisch verwijderd. Hulp bij het ontwerp of de uitrol? Mail ralph@rkpc.be of kijk op rkpc.be.