Tetra Industriële Security

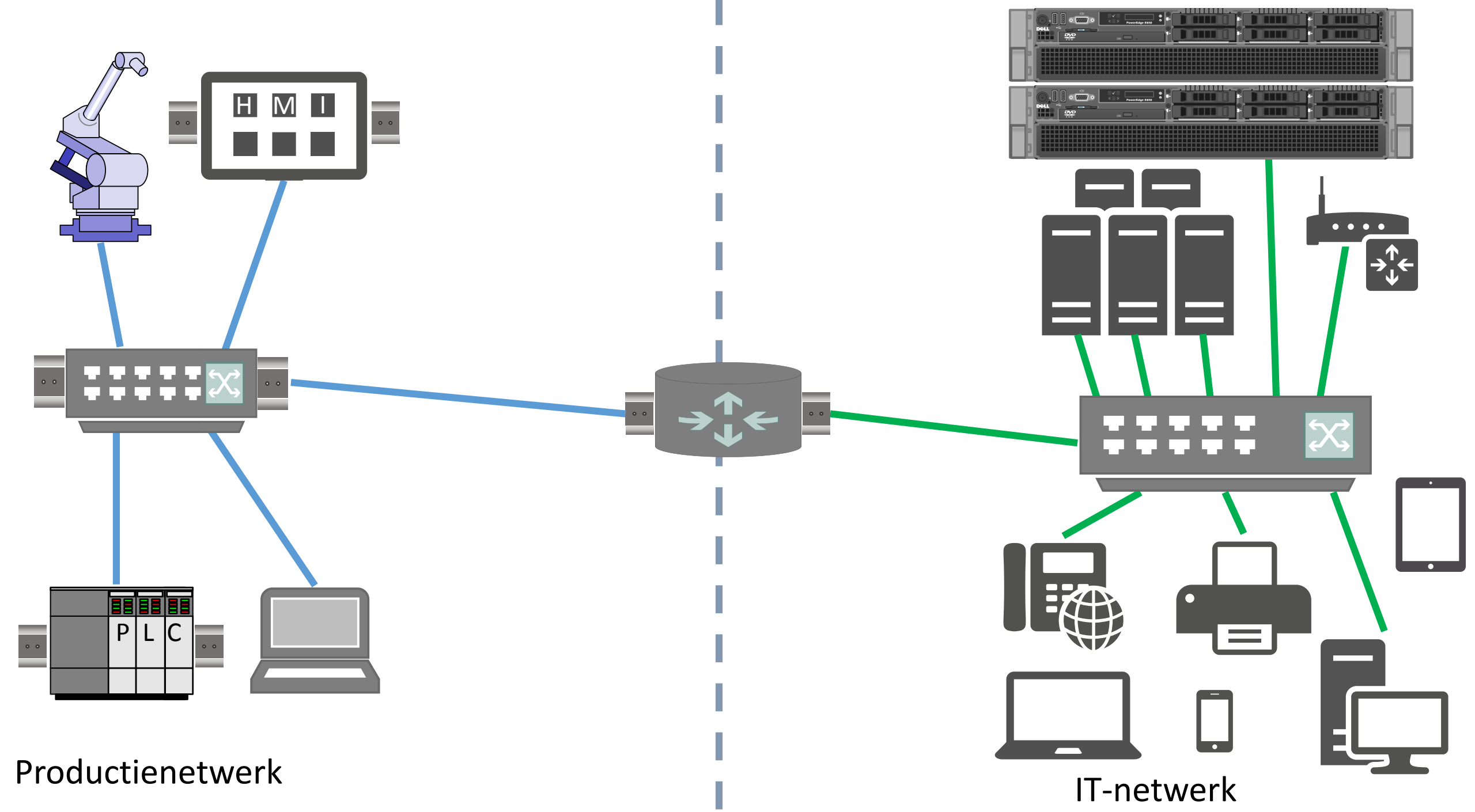
Gebruikersgroep

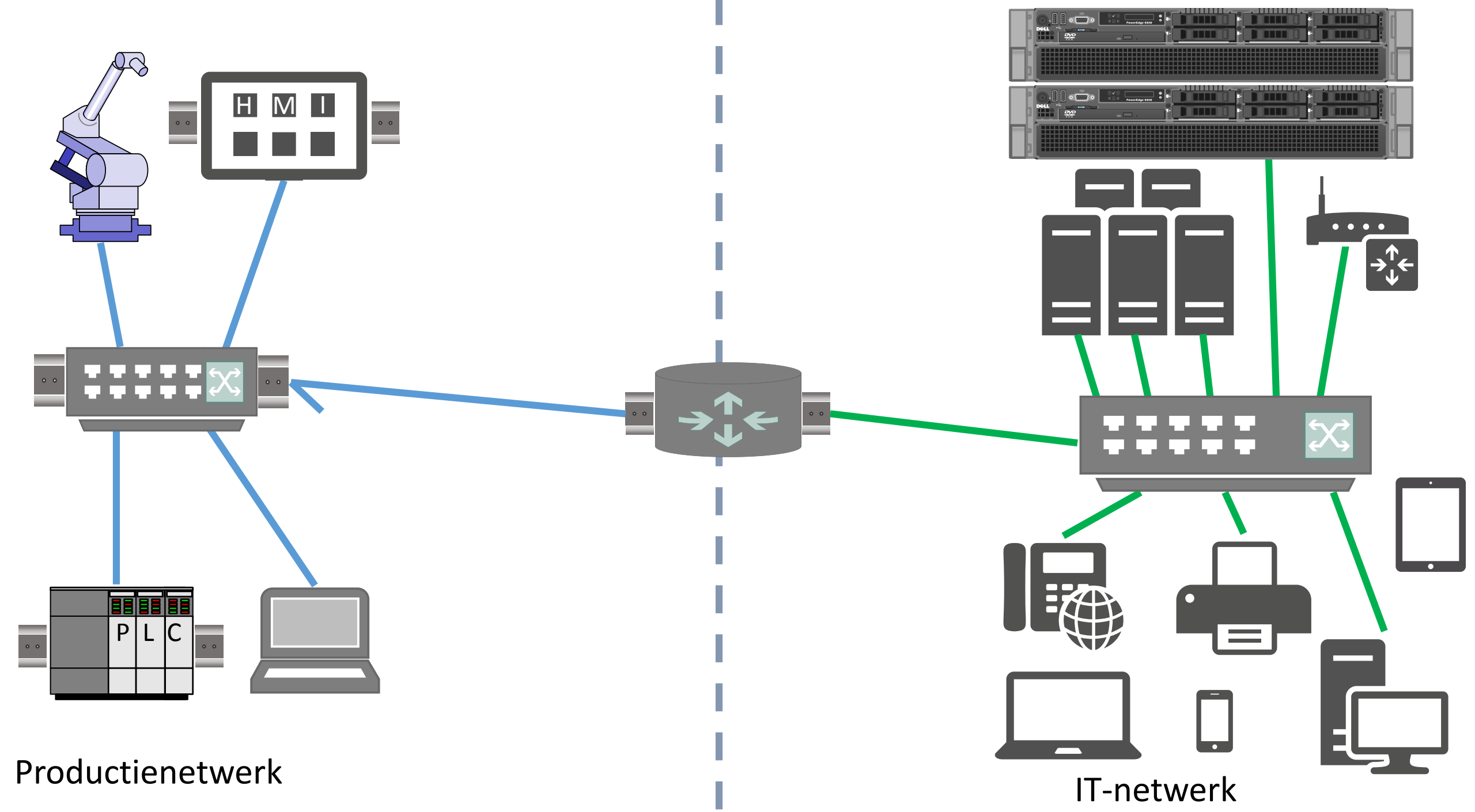
07 / 05 / 2015

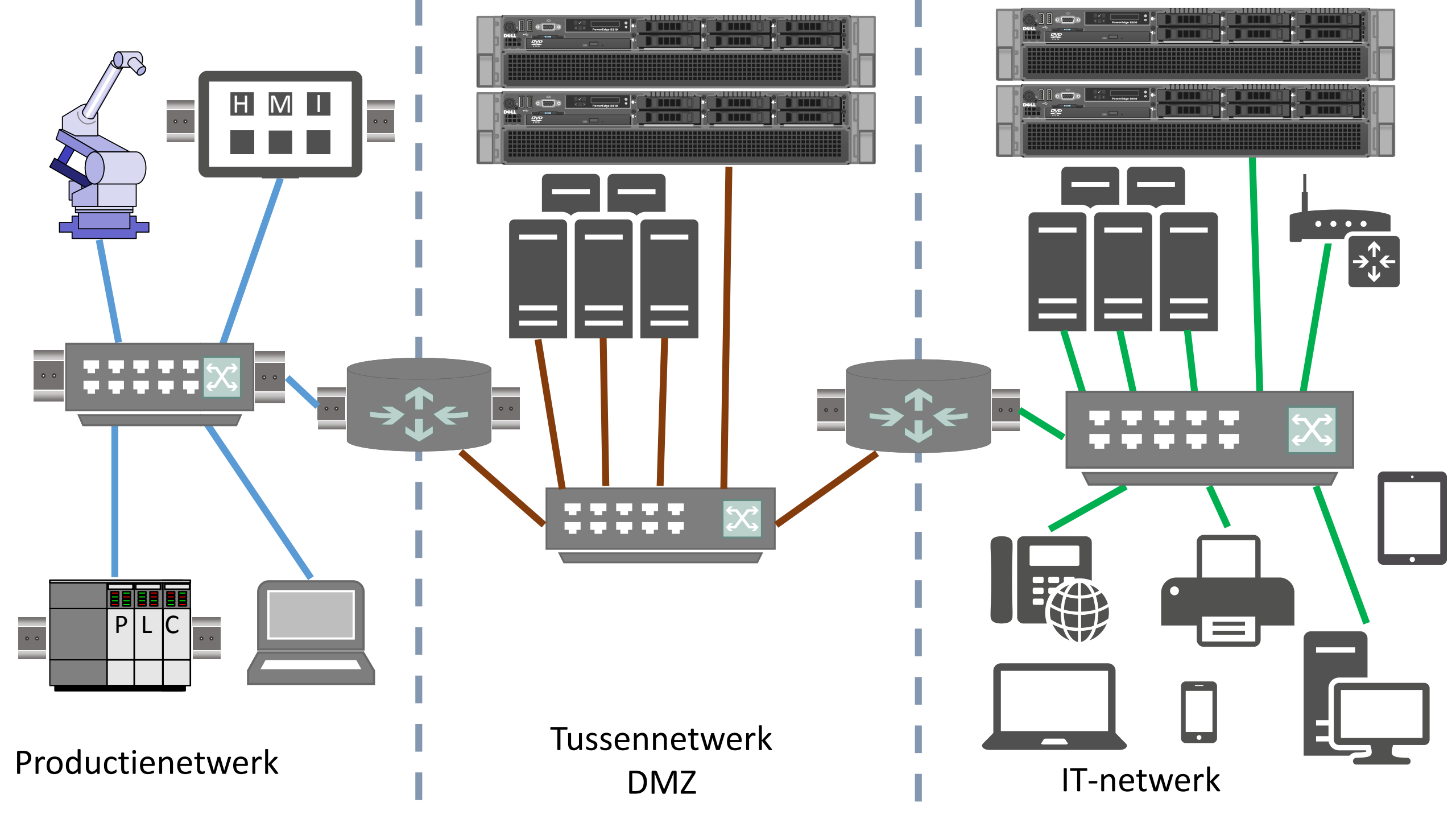
Netwerkarchitectuur

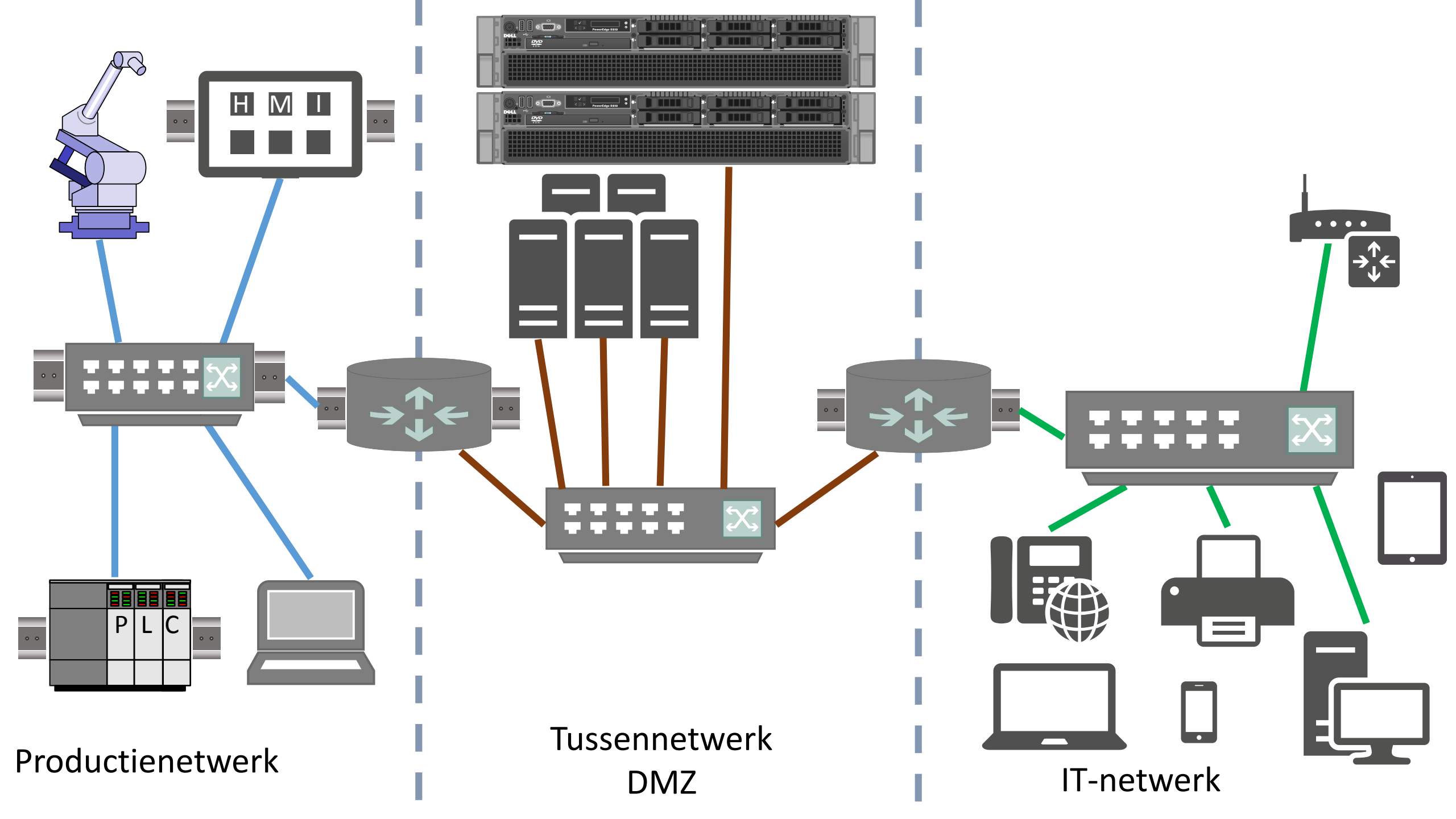
Remote Access

Specifieke onderzoekspistes


H M I
P L C
Productienetwerk
IT-netwerk


H M I
P L C
Productienetwerk
IT-netwerk

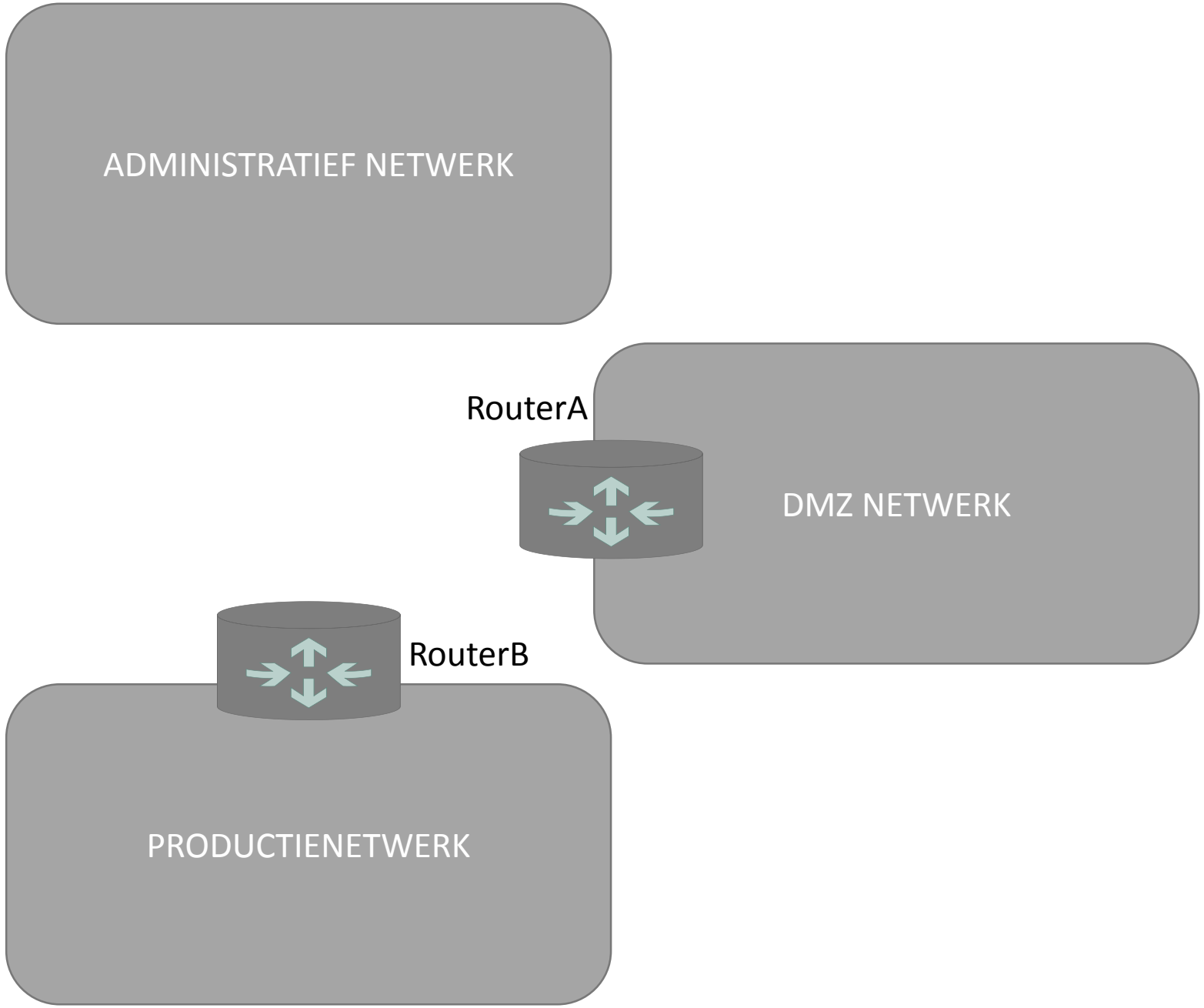

H M I
P L C
Productienetwerk
Tussennetwerk
DMZ
IT-netwerk


H M I
P L C
Productienetwerk
Tussennetwerk
DMZ
IT-netwerk

Scenario

Vraag: bepaalde toestellen uit het PRODUCTIEnetwerk bereiken voor het ADMINISTRATIEF netwerk / DMZ

Antwoord: diverse manieren:
- 1:1 NAT (range)
- 1:1 NAT (device)
- Port Forwarding
- VPN
- (VLAN)



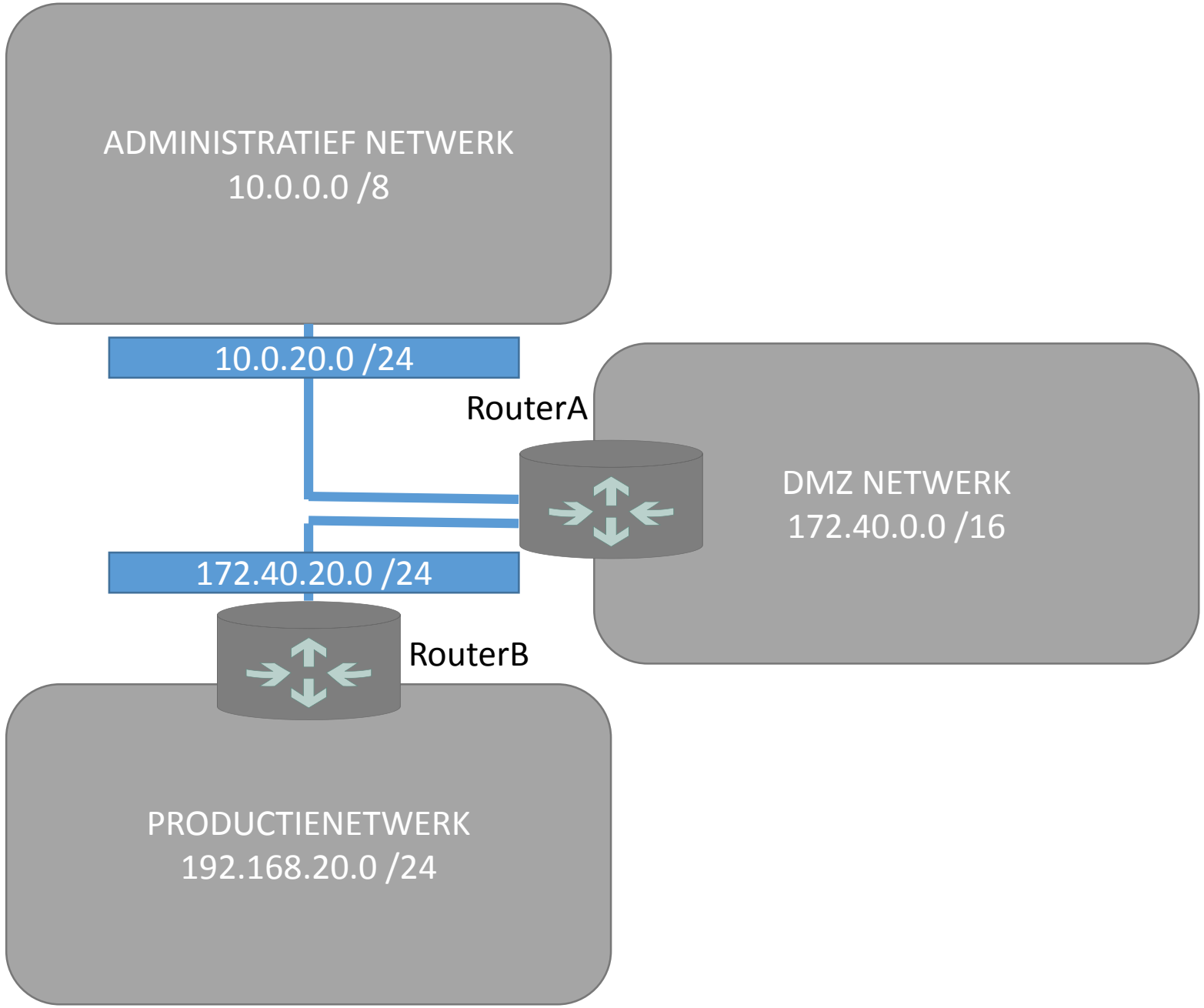
1:1 NAT (range)

Stel in op *RouterB*:
1:1 NAT
van 192.168.20.0 /24
naar 172.40.20.0 /24
Stel in op *RouterA:*
1:1 NAT
van 172.40.20.0 /24
naar 10.0.20.0 /24

Op die manier is bijv. toestel 192.168.20.15 transparant bereikbaar via adres 172.40.20.15 én via adres 10.0.20.15
… en zo ook alle andere 254 adressen

-> Althans op IP niveau (Layer3),
niet MAC (Layer2)

-> Groot veiligheidsrisico, firewalls worden hierdoor omzeild



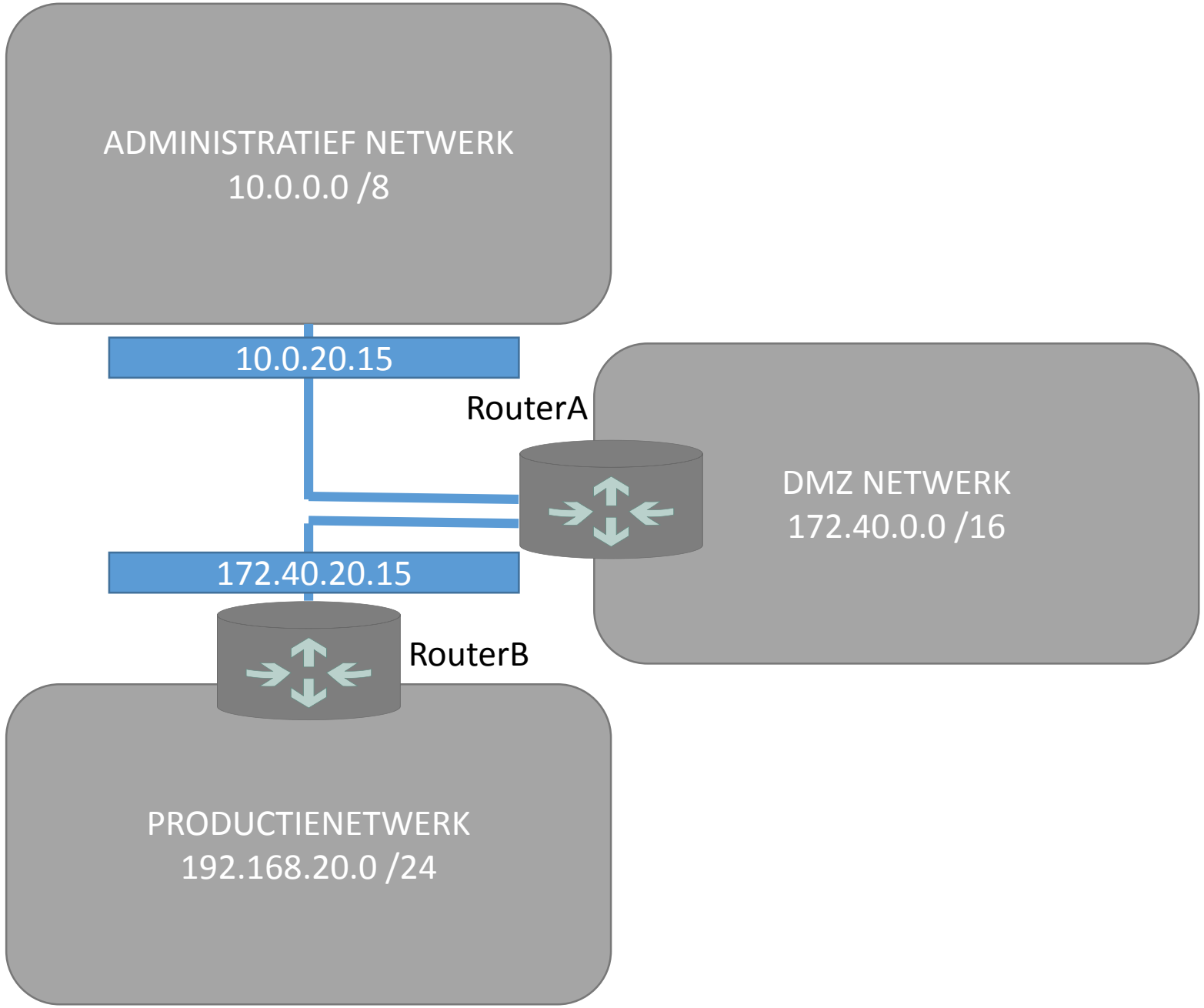
1:1 NAT (Device)

Stel in op *RouterB*:
1:1 NAT
van 192.168.20.15
naar 172.40.20.15
Stel in op *RouterA*:
1:1 NAT
van 172.40.20.15
naar 10.0.20.15

Op die manier is enkel toestel 192.168.20.15 transparant bereikbaar via adres 172.40.20.15 en via adres 10.0.20.15

-> Althans op IP niveau (Layer3),
niet MAC (Layer2)

-> Nog steeds veiligheidsrisico, firewalls worden hierdoor omzeild

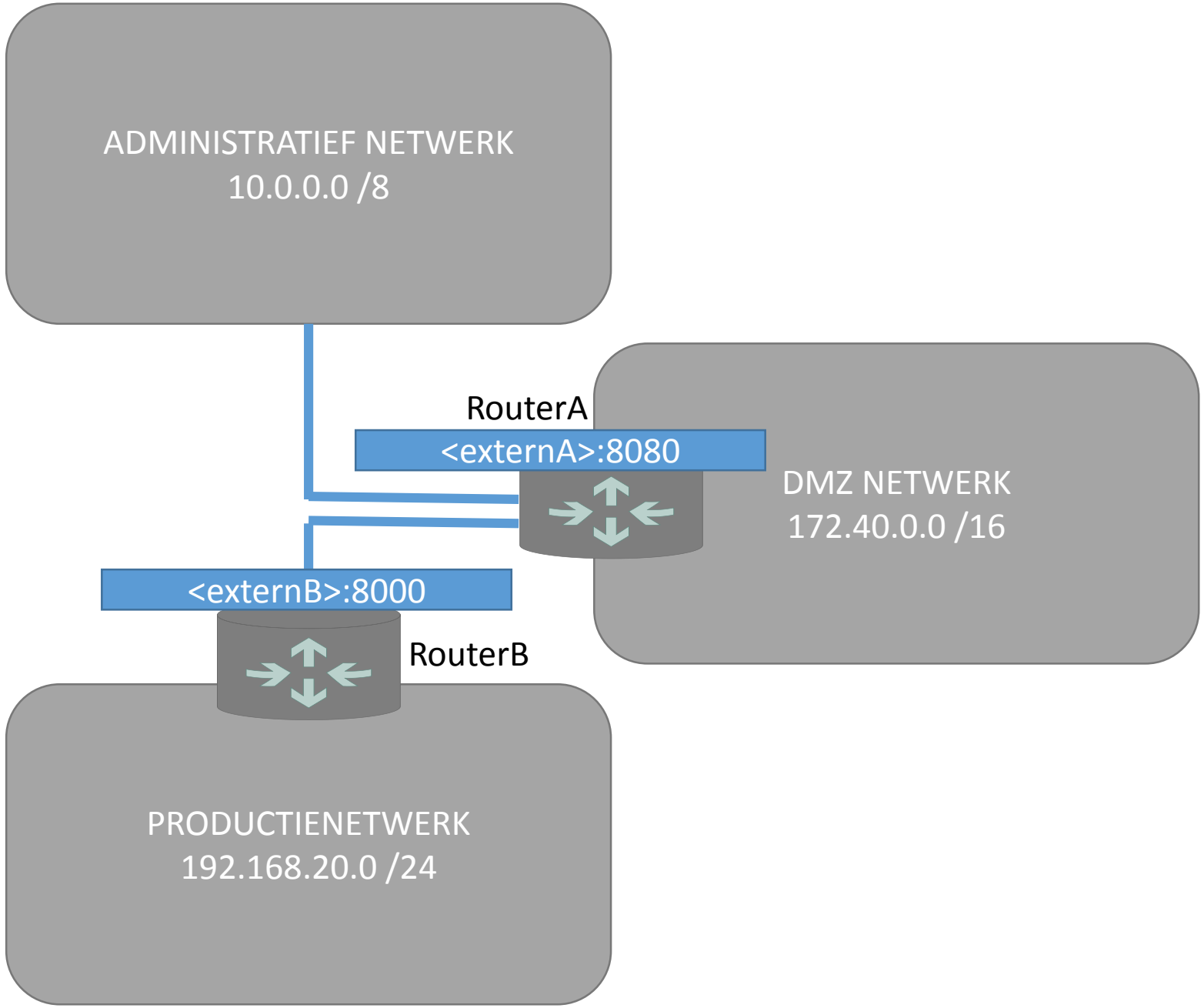


Port Forwarding

Stel in op *RouterB*:
Port Forward
van <externB> poort 8000
naar 192.168.20.15 poort 80
Stel in op *RouterA*:
Port Forward
van <externA> poort 8080
naar <externB> poort 8000

Op die manier is enkel poort 80 van toestel 192.168.20.15 bereikbaar door naar de *routerB* te connecteren op poort 8000
of *routerA* op poort 8080

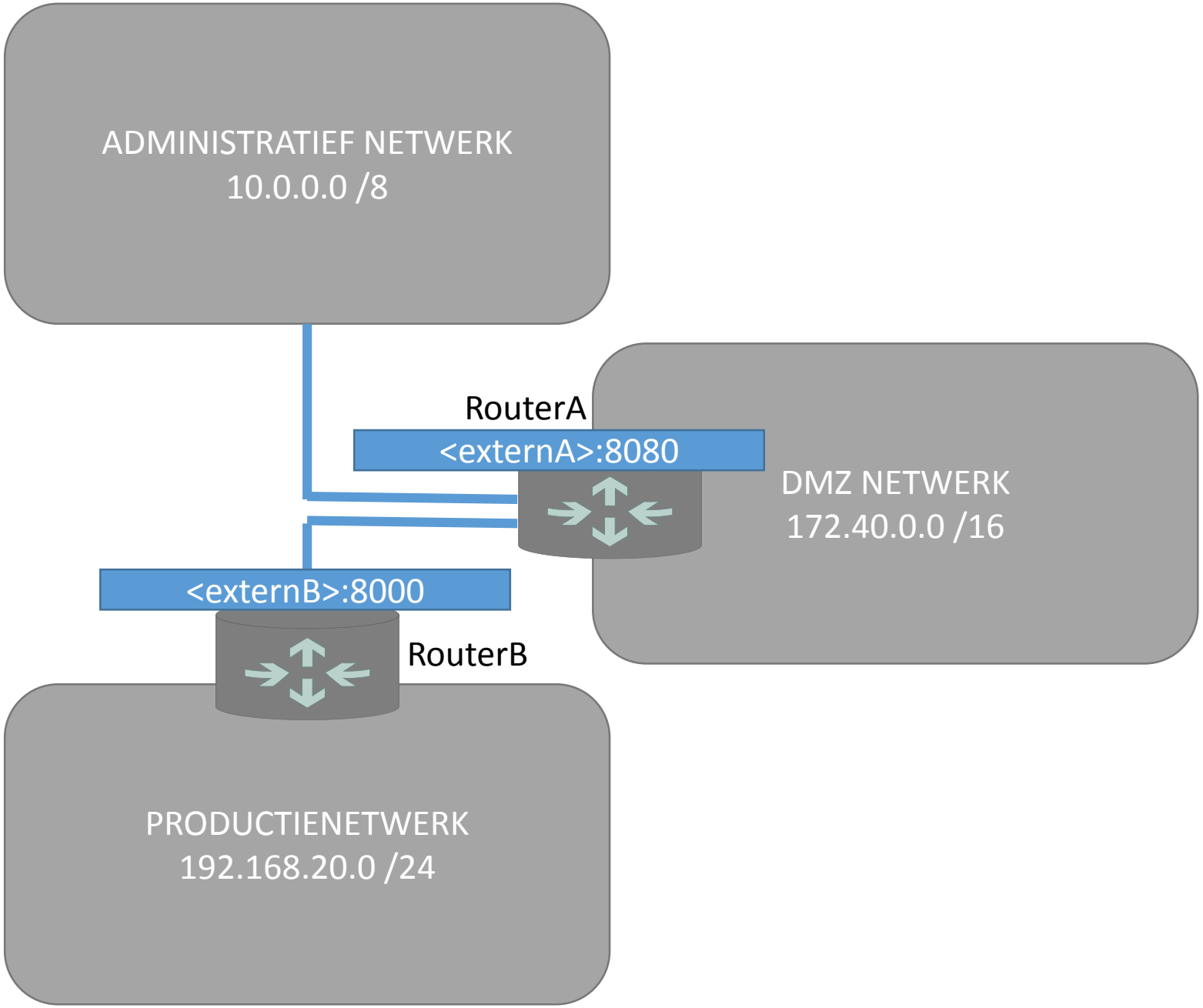
-> Meestal kan hier bijkomstig het bron IP bij gekozen worden (hogere beveiliging)
-> Althans op IP niveau (Layer3), niet MAC (Layer2)
-> Kleiner veiligheidsrisico, *RouterB* wordt hierdoor omzeild



1:1 NAT (range)
1:1 NAT (Device)
Port Forwarding

ONDERZOEKSPISTES:
Routeerbaarheid van protocollen
- modbusTCP, Profinet, e.a ?

Beïnvloeding performantie?



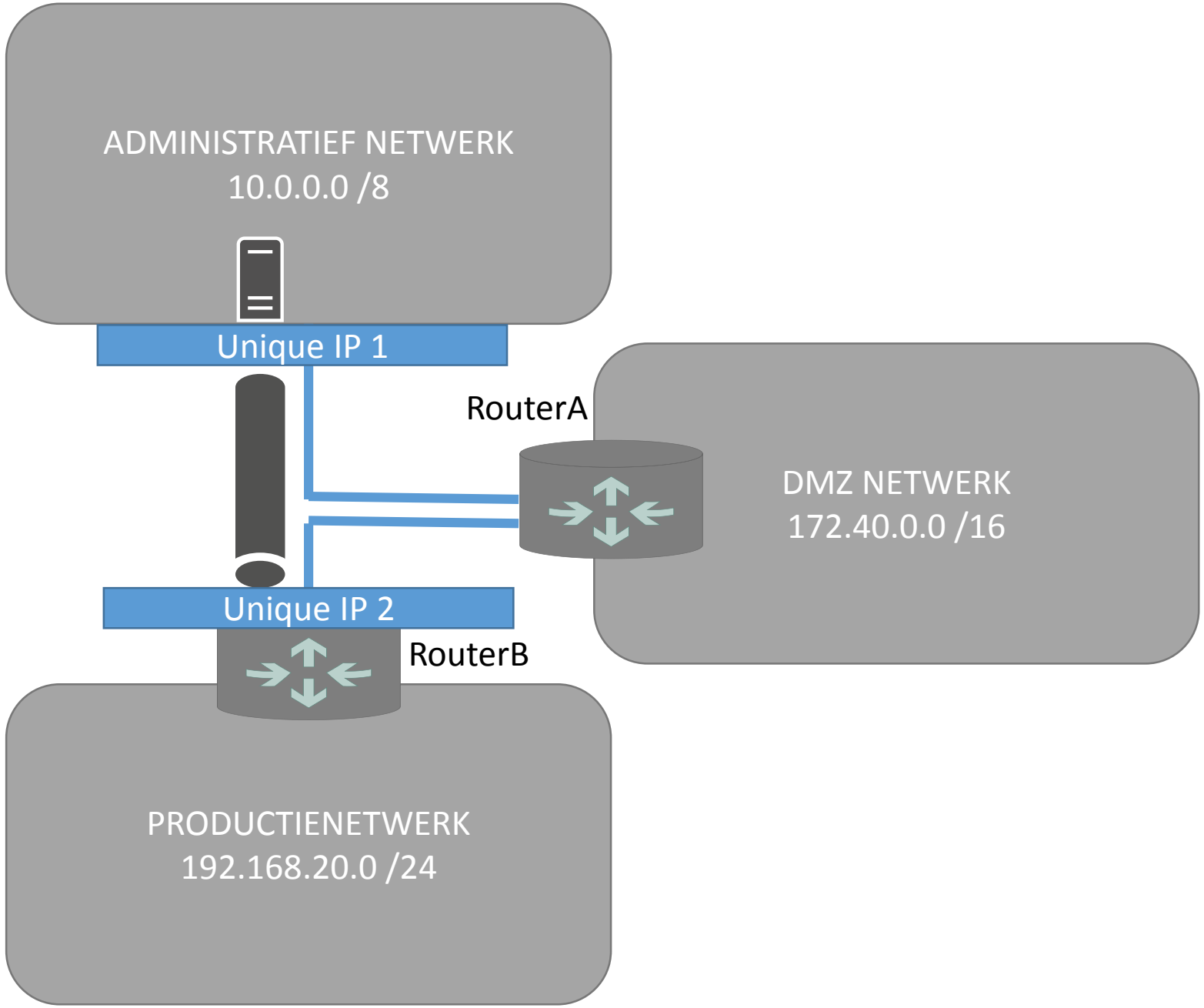
VPN

Veel VPN oplossingen zijn niet ontwikkeld uit veiligheid, maar om een oplossing voor afstandsbeheer te ontwikkelen.
De veiligste oplossing is het gebruik van **ondertekende certificaten**.

Onderteken (of laat ze ondertekenen) door een zogenaamde *Certificate Authority* (CA): zowel een server als een client certificaat.

Importeer op een *veilige* manier het private server certificaat plus het publieke client certificaat op RouterB.
Gebruik dan Windows software (bijv. OpenVPN) om op de client hetzelfde te doen: publieke server certificaat en private client certificaat.

-> Nog steeds enkel IP niveau (Layer3)
-> Heel wat configureerwerk en voor elke client te herhalen

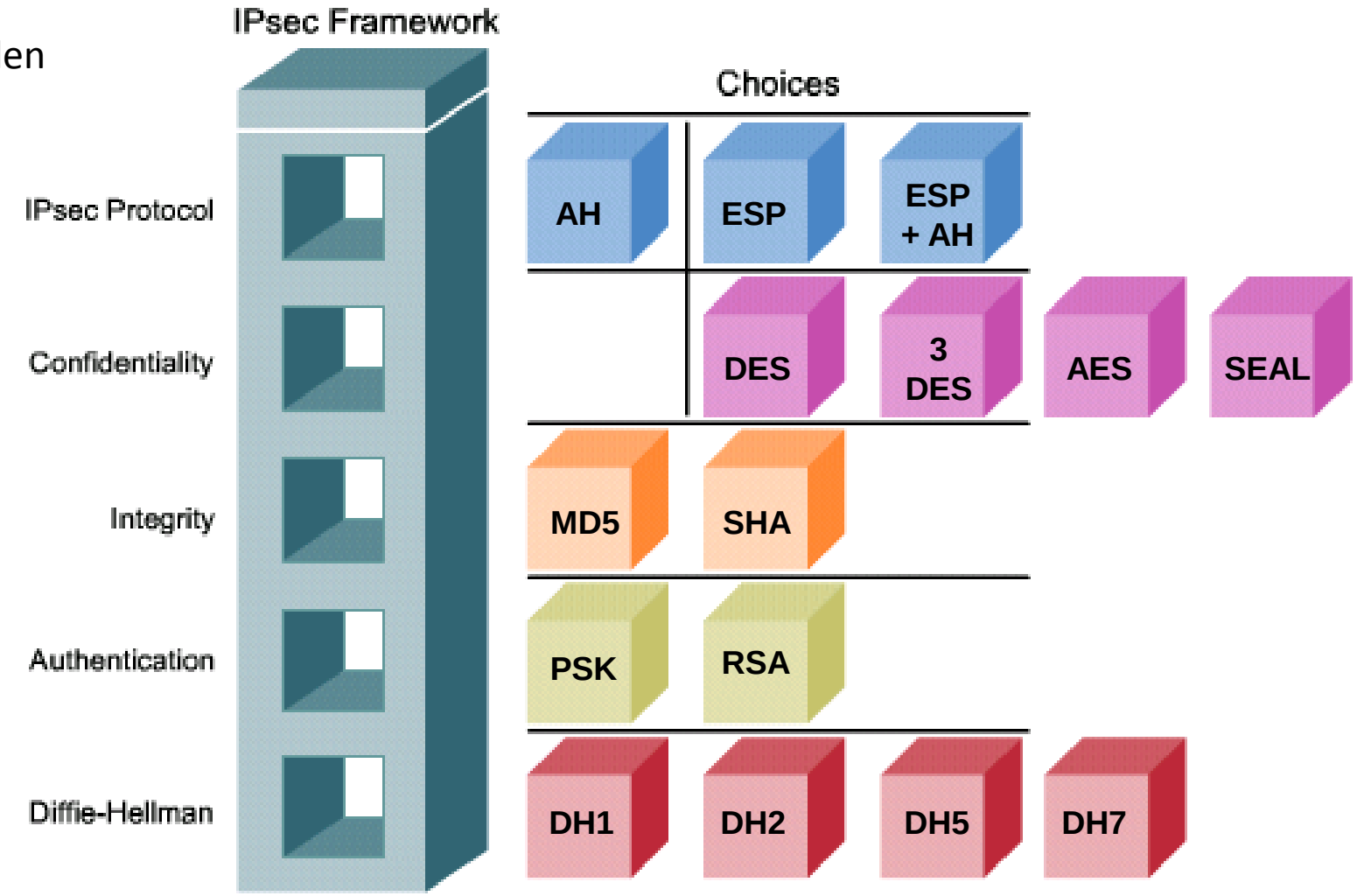


VPN opties

ONDERZOEKSPISTES:
Encapsuleerbaarheid van protocollen
- modbusTCP, Profinet, e.a?

Beïnvloeding performantie?

VPN op veilige manier opzetten?
Mogelijke (veiligste) keuzes?

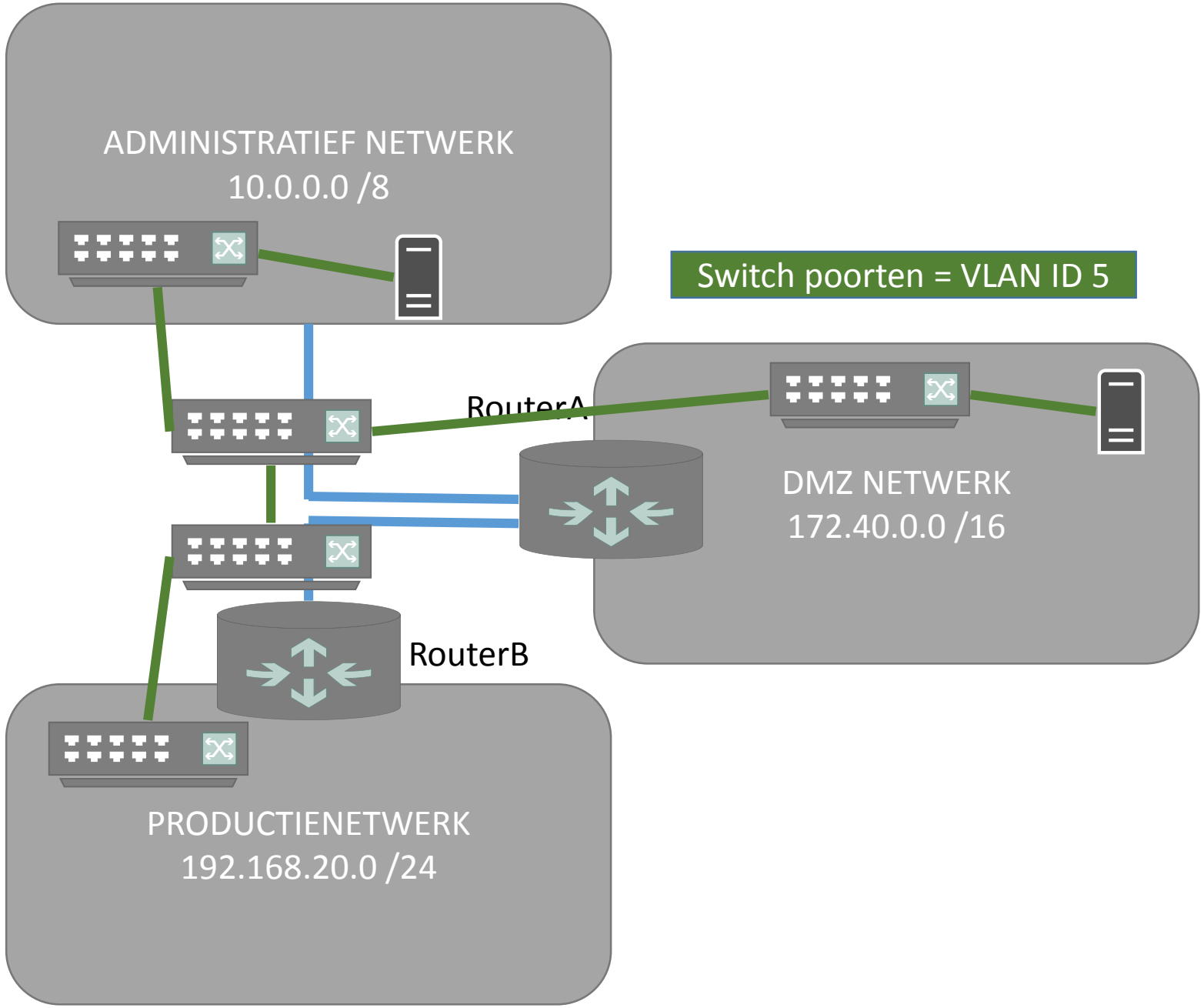


VLAN

Layer 2 protocol en dus niet mogelijk doorheen routers, het moet gezien worden als een *extensie* van een bepaald netwerk die via switches zich uitstrekt tot een bepaald netwerk of device.

Meestal worden VLANS gebruikt als ***alternatief*** voor routers. Het routering gedeelte wordt dan namelijk op administratief netwerk niveau gedaan.

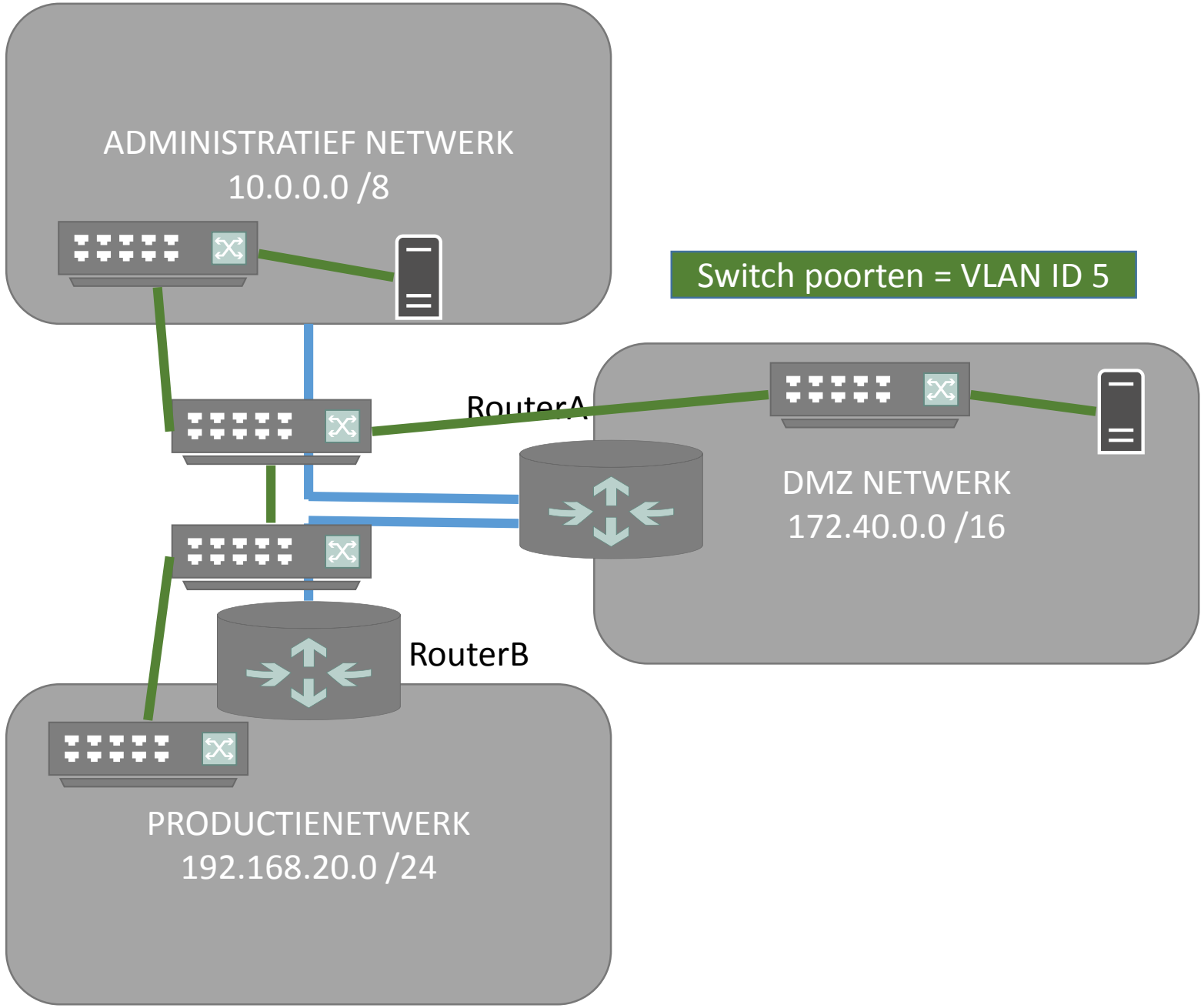
-> Layer2 niveau
-> Behoorlijke architectuur impact



VLAN

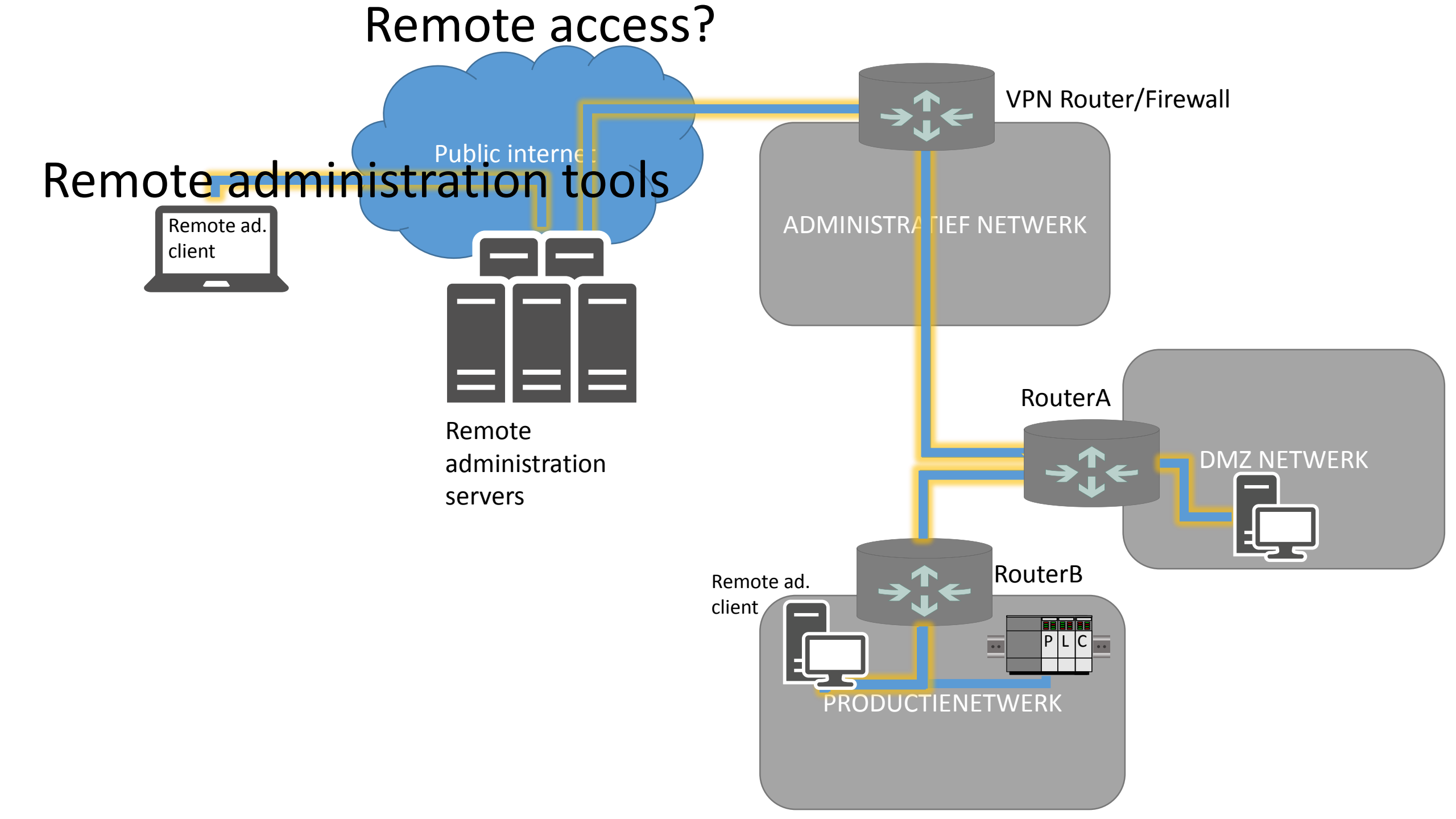
ONDERZOEKSPISTES:
Encapsuleerbaarheid van protocollen
- modbusTCP, Profinet, e.a?

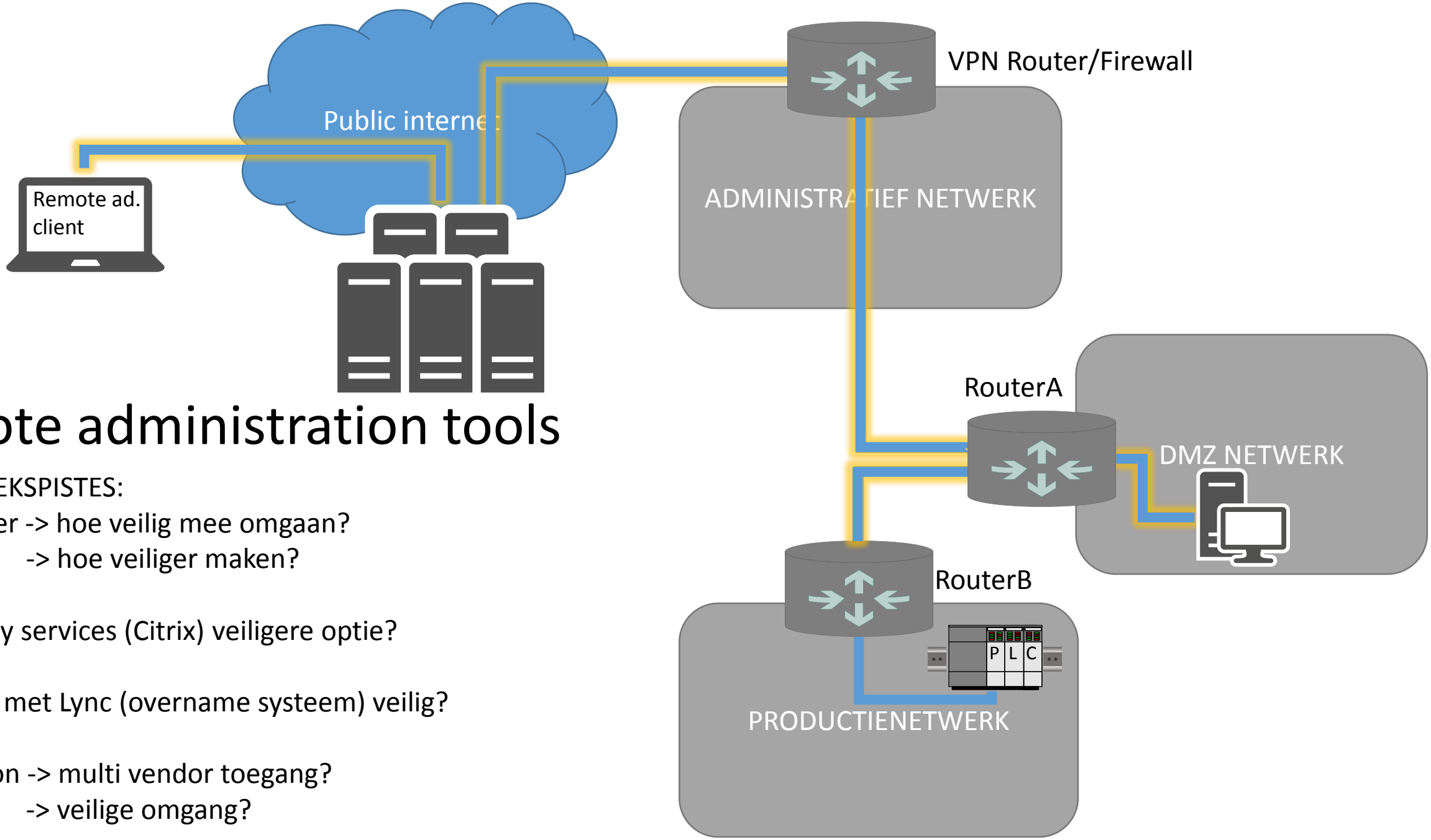
Performantie?



Remote access?

Remote administration tools





Remote administration tools

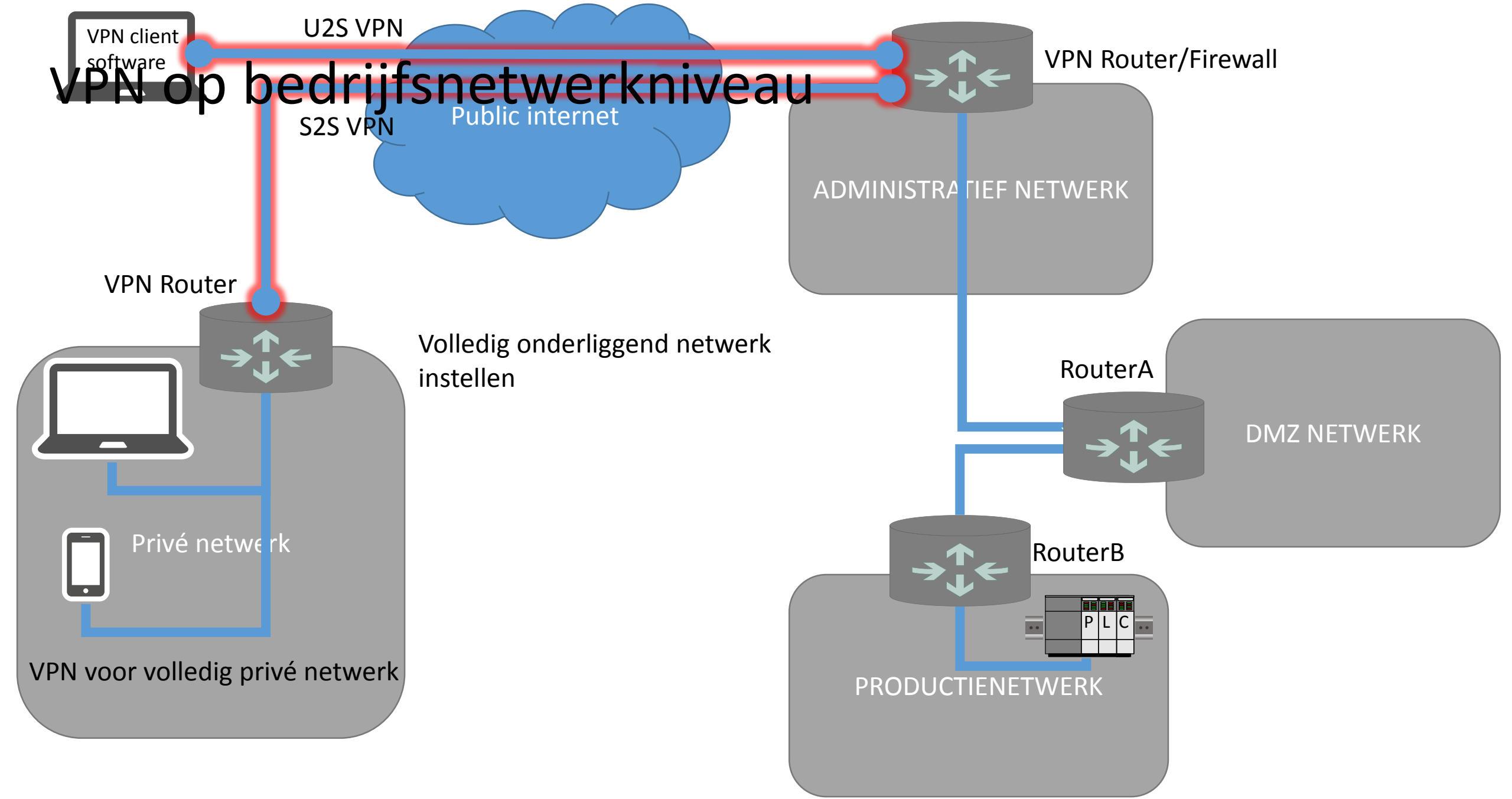
ONDERZOEKSPISTES:
Teamviewer -> hoe veilig mee omgaan?
-> hoe veiliger maken?

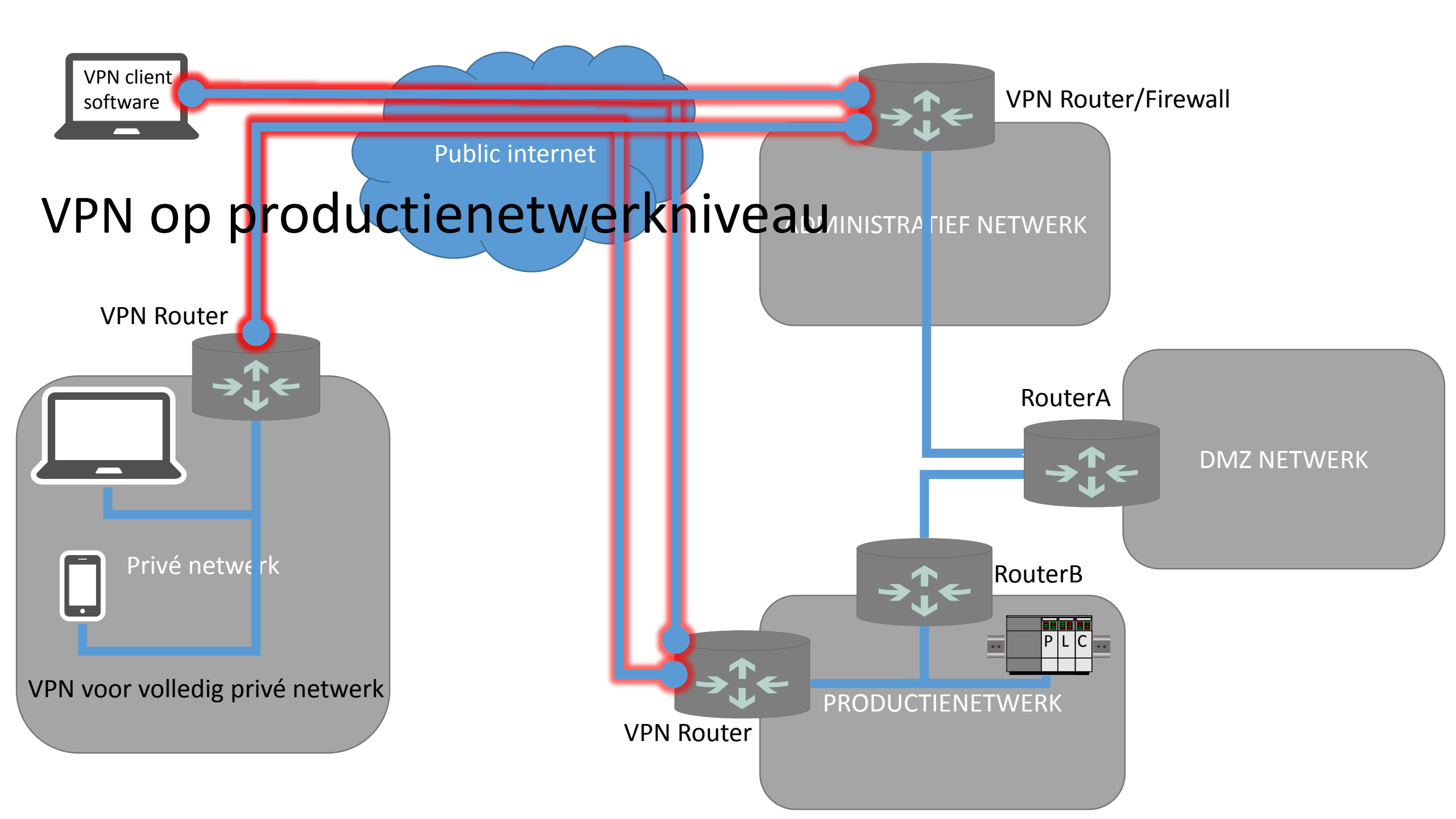
RD gateway services (Citrix) veiligere optie?

Office 365 met Lync (overname systeem) veilig?

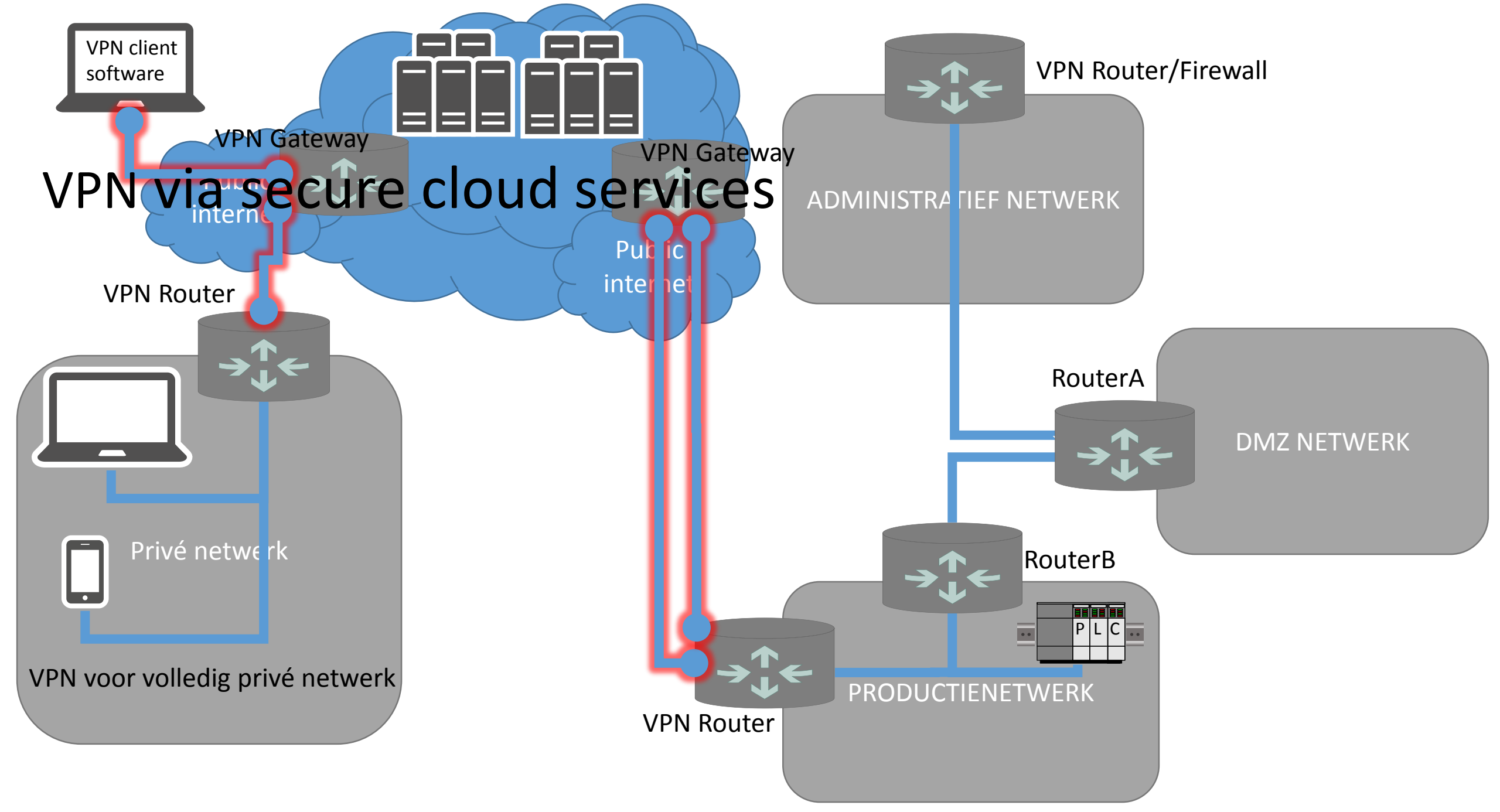
Jumpstation -> multi vendor toegang?
-> veilige omgang?

VPN op bedrijfsnetwerkniveau

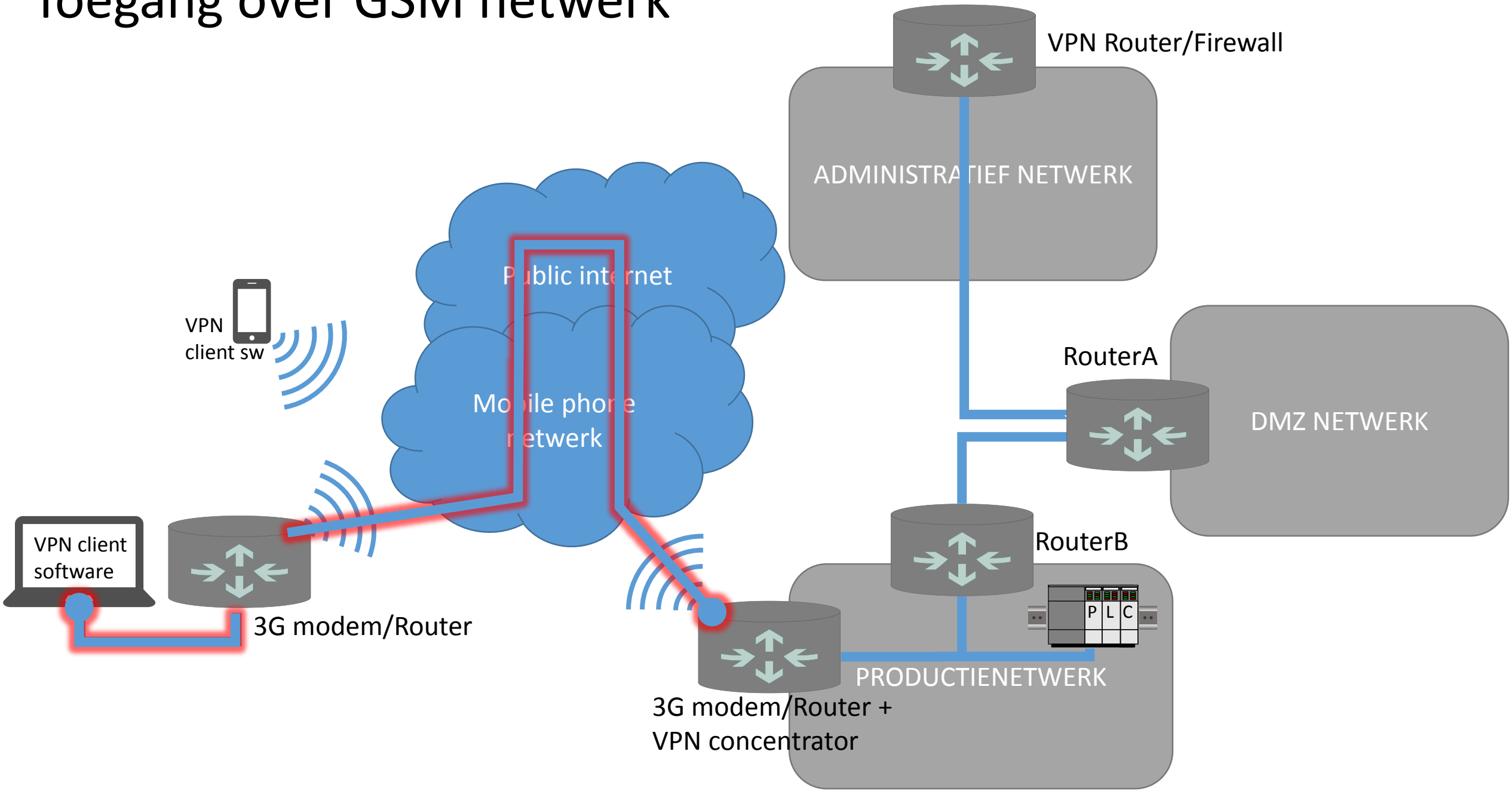



VPN client software
Public internet
VPN Router/Firewall
VPN op productienetwerkniveau
ADMINISTRATIEF NETWERK
VPN Router
RouterA
DMZ NETWERK
Privé netwerk
RouterB
P L C
VPN voor volledig privé netwerk
PRODUCTIENETWERK
VPN Router

VPN via secure cloud services



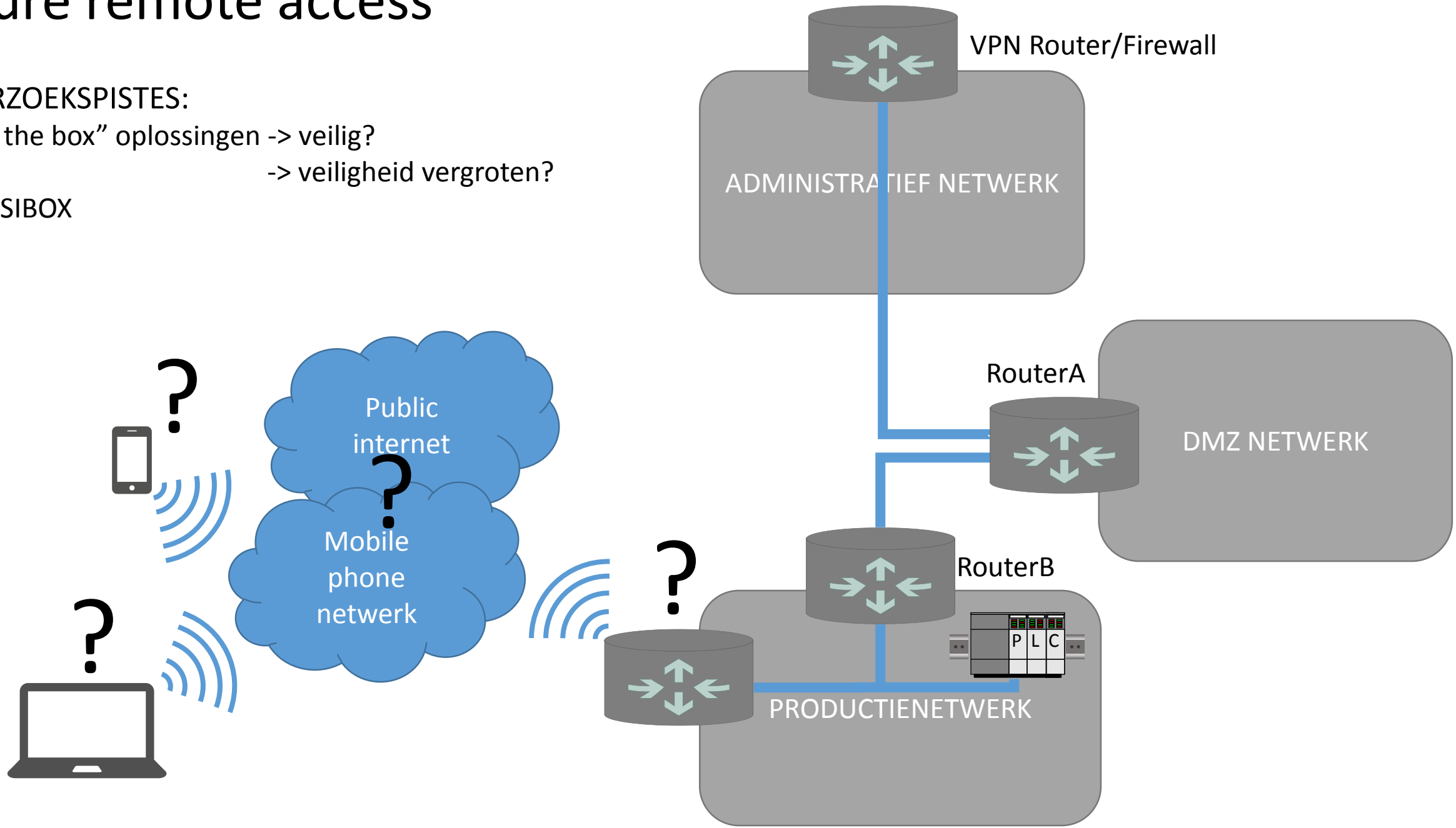
Toegang over GSM netwerk



Secure remote access

ONDERZOEKSPISTES:
“Out of the box” oplossingen -> veilig?
-> veiligheid vergroten?

bvb. TOSIBOX



Bijkomende mogelijke onderzoekspistes

- Cisco Industrial t.o.v. Siemens, Beckhoff, Phoenix Contact
- Specifiek onderzoek naar bedrijfszekerheid van Profisafe
- Transparante firewalls (Hirschmann Tofino, mGuard Stealth mode)
- Veiligheid eWon?

Awareness en Opleidingen

- Basiscursus netwerken (OT)
  - Ethernet
  - TCP/IP
  - …
- Basiscursus industriële netwerken (IT)
  - AIC vs CIA
  - Industriële producten
  - Profinet, Ethercat, Modbus TCP
  - …
- Cursus awareness en security basics
  - Kwetsbaarheden en mogelijke gevolgen
  - Basic guidelines: bvb. default users wissen, omgaan met paswoorden…
  - Demo’s
  - …