VNG LAN infrastructuur
High-level ontwerp

02-08-2020

Inhoudsopgave

Documentbeheer

Versiebeheer

Versie	Datum	Omschrijving	auteur
0.1	09-07-2020	Eerste draft	Wil Hesen
0.2	16-07-2020	Feedback update	Wil Hesen
1.0	11-08-2020	Feedback verwerkt	Arjan Regtien

Reviews

Versie	Datum	Naam	Functie	Bedrijf
0.1	14-07-2020	Benito Deekman	Netwerk engineer	Routz
0.1	16-07-2020	Roland Lemmerlijn	Team Manager	Valid

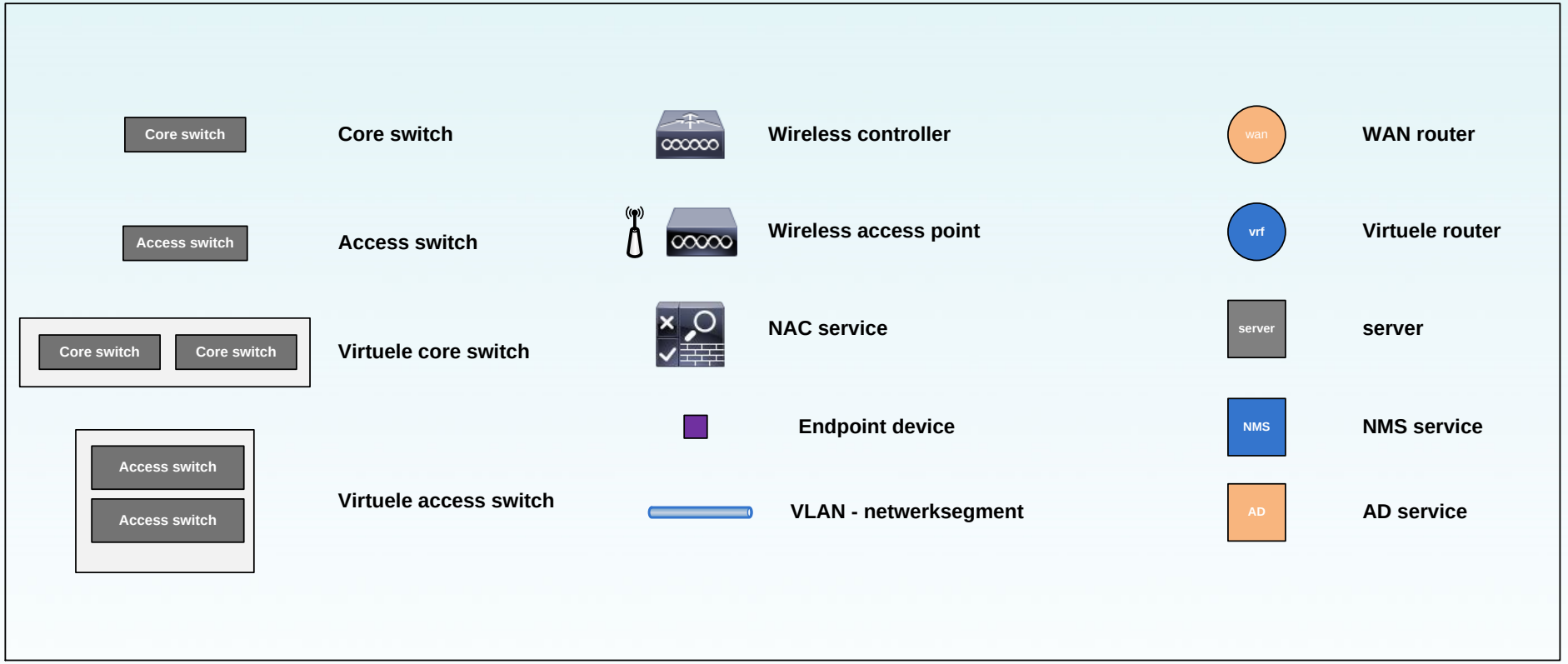
Afkortingen

Afkorting	Betekenis
AAA	Authenticatie Autorisatie Accounting
AD	Active directory
BGP	Border Gateway Protocol
CAPWAP	Control And Provisioning of Wireless Access Points
CIS	Center for Internet Security
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
GGI	Gemeentelijke Gemeenschappelijke Infrastructuur
IPAM	IP Address Management
LAN	Local Area Network
NAC	Network Access control

Afkortingen

Afkorting	Betekenis
NMS	Netwerk Management systeem
NTP	Network Time Protocol
MEC	MultiChassis EtherChannel
MER	Main Equipment Room
NFV	Network Function virtualization
QoS	Quality of Service
SAAS	Software As A Service
SFP	Small Form-factor Pluggable
SER	Satellite Equipment Room
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network

Legenda


Core switch
Core switch
Access switch
Access switch
Core switch
Core switch
Virtuele core switch
Access switch
Access switch
Virtuele access switch
Wireless controller
Wireless access point
NAC service
Endpoint device
VLAN - netwerksegment
wan
WAN router
vrf
Virtuele router
server
server
NMS
NMS service
AD
AD service

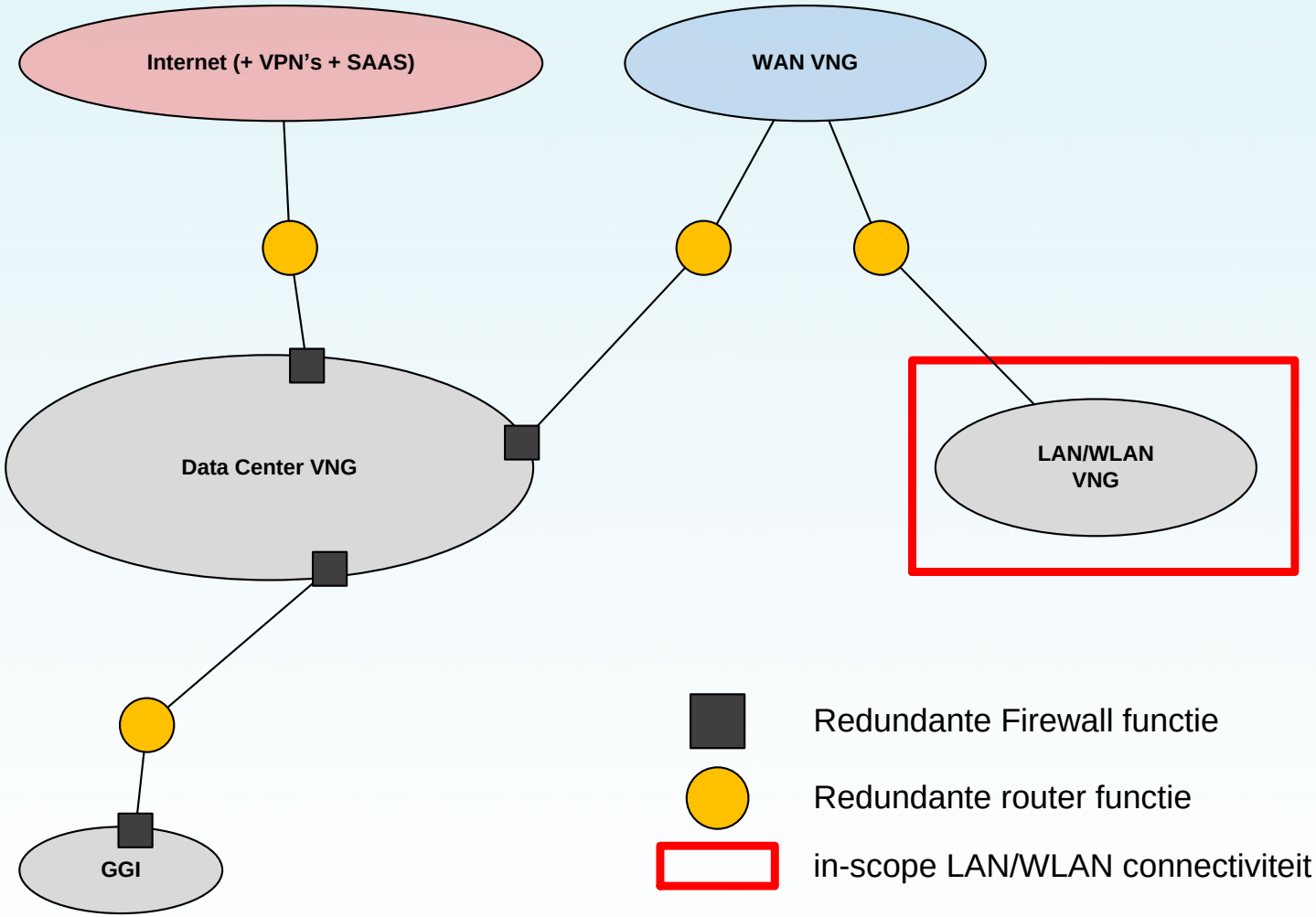
Scope

Scope

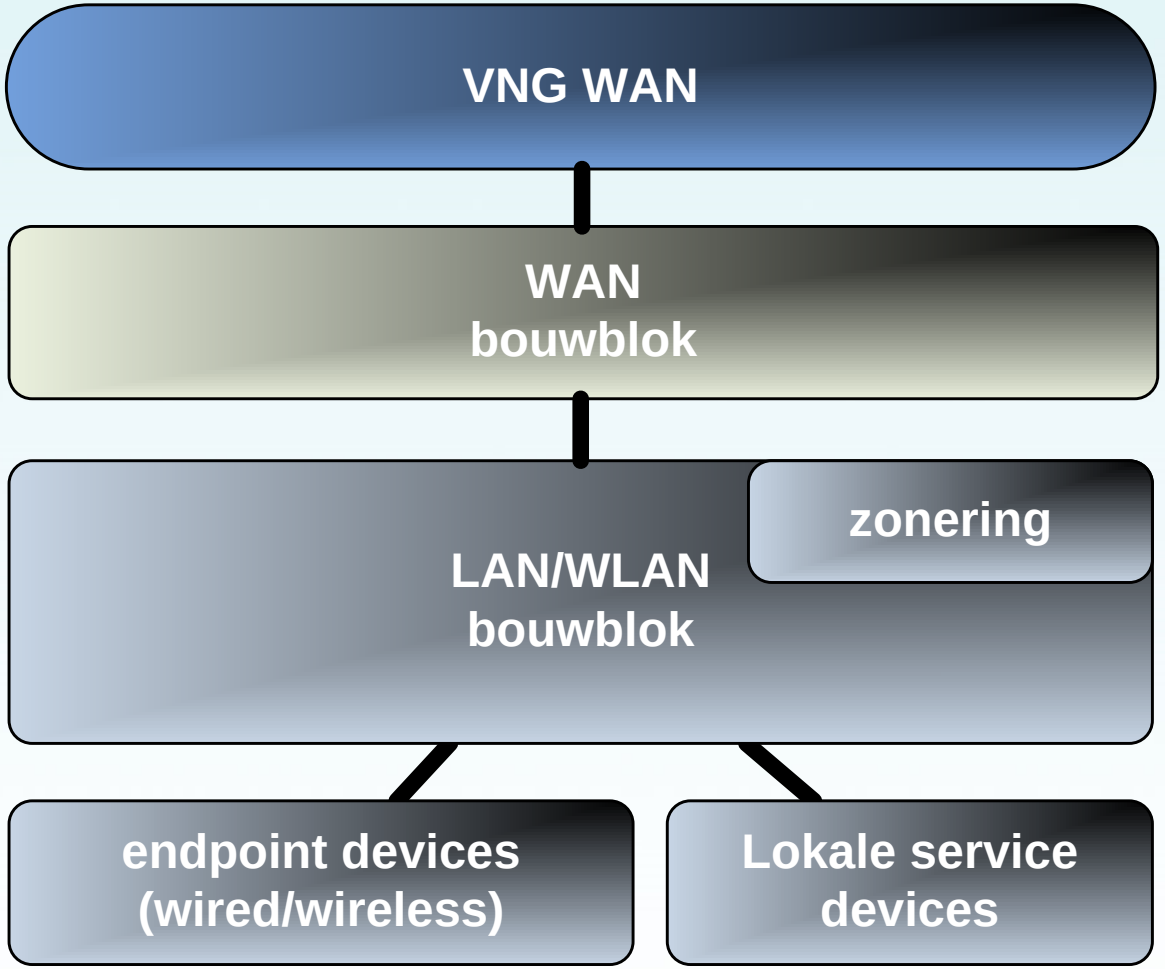
- De LAN/WLAN netwerkinfrastructuur van de locatie Willemshof van VNG;
- Lokale services die ingezet kunnen worden binnen deze locatie;
- Beveiligingsaspecten als netwerkzonering, hardening en NAC service;
- De centrale services die van toepassing zijn voor de connectiviteit met een locatie van VNG;
- De centrale services die van toepassing zijn voor het beheer van een locatie van VNG.

Infrastructuur

Overzichtsplaat



Bouwblokken



Bouwblokken

Ontwerpkeuze: Het LAN/WLAN bouwblok voorziet in netwerkzonering
- **Rationale** (waarom)
  - Voorzien in logische scheiding van functionaliteit
  - Voorzien in beveligingsfunctie per netwerkzone
- **Implicatie** (hoe)
  - Zonering gebaseerd op VLAN's
  - Beveiliging gebaseerd op ACL's

Ontwerpkeuze: Het WAN bouwblok voorziet in dynamische uitwisseling van IP blokken
- **Rationale** (waarom)
  - Voorzien in end-to-end IP connectiviteit
  - Voorzien in dynamische aanpassing bij wijzigingen
- **Implicatie** (hoe)
  - Uitwisseling van IP blokken gebaseerd op het BGP protocol

Ontwerpkeuze: Het bouwblok voor endpoint devices voorziet in netwerkconnectiviteit voor de wired en wireless endpoint devices
- **Rationale** (waarom)
  - Voorzien in standaard koppelvlak voor wired eindpoint devices
  - Voorzien in standaard koppelvlak voor wireless devices
- **Implicatie** (hoe)
  - Dit bouwblok is geïntegreerd binnen het LAN/WLAN bouwblok
  - De wired endpoint devices worden direct gekoppeld met dit bouwblok
  - De wireless endpoint devices worden via een AP gekoppeld met dit bouwblok

Bouwblokken

Ontwerpkeuze: Het bouwblok voor lokale service devices voorziet in netwerkconnectiviteit voor compute, storage en netwerk devices

Rationale (waarom)

Voorzien in standaard koppelvlak voor compute, storage en netwerk devices

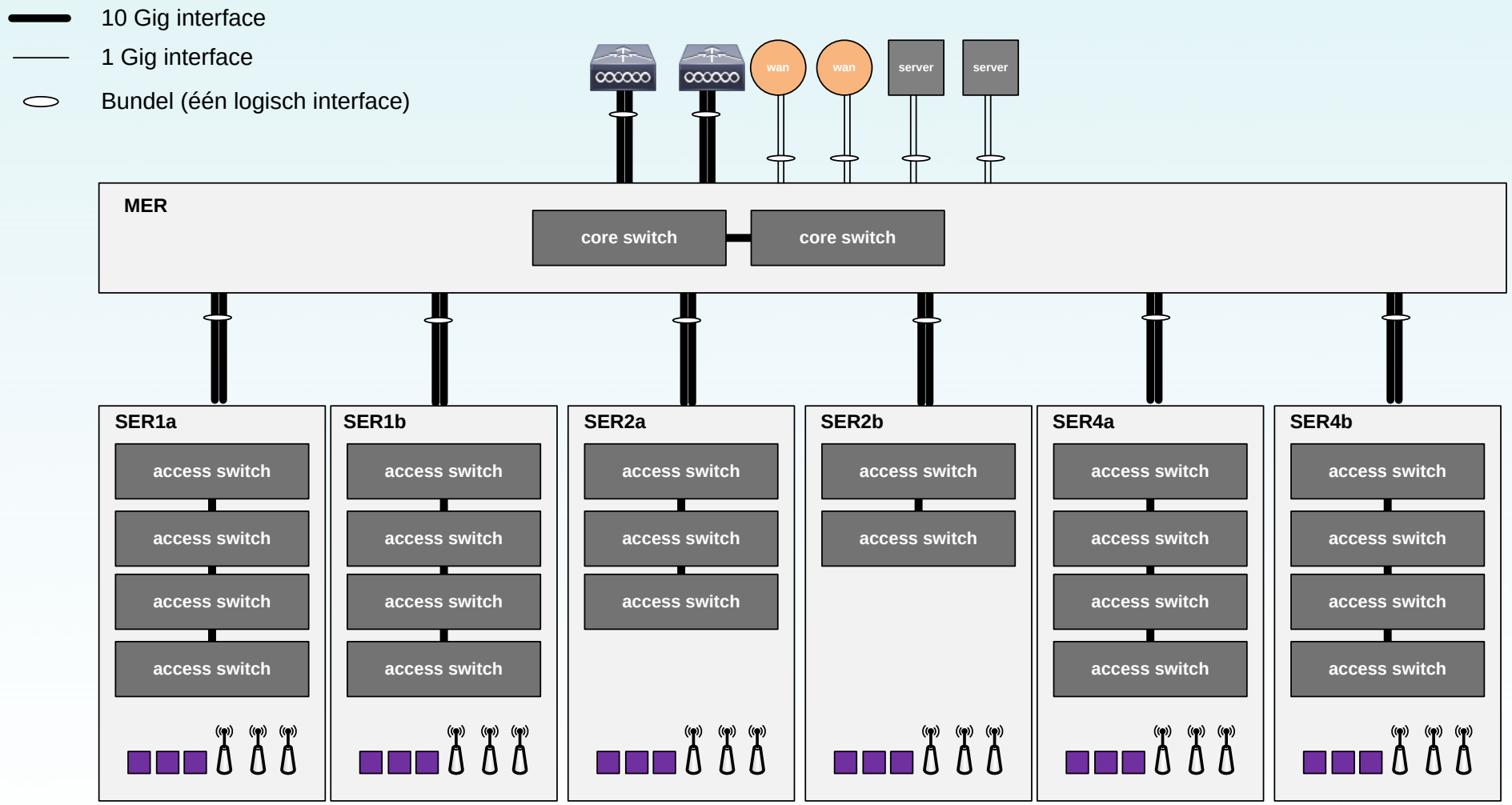
Implicatie (hoe)

Dit bouwblok is geïntegreerd binnen het LAN/WLAN bouwblok

Lokale compute devices worden gekoppeld met dit bouwblok

De WLAN controllers en WAN devices worden gekoppeld met dit bouwblok

LAN infrastructuur fysiek



LAN infrastructuur fysiek

Ontwerpkeuze: De LAN infrastructuur is gebaseerd op een collapsed core model
- **Rationale** (waarom)
  - Voorzien in hoge beschikbaar
  - Voorzien in schaalbaarheid
  - Voorzien in core–laag voor snelle doorvoer van end-to-end connectiviteit
  - Voorzien in distributie-laag voor koppelen van de afzonderlijke access-lagen
  - Voorzien in server-laag voor koppelen van lokale services
  - Voorzien in access-laag voor koppelen van endpoint devices en access-points
- **Implicatie** (hoe)
  - De core-, distributie- en server-laag zijn geconsolideerd binnen één laag
  - Elke SER heeft zijn eigen access-laag - elk afzonderlijk gekoppeld met de distributie-laag

Ontwerpkeuze: De core-laag bestaat uit 2 core switches geïmplementeerd als één logische switch
- **Rationale** (waarom)
  - Voorzien in hoge beschikbaar
  - Voorzien in loopvrij laag-2 netwerk
  - Voorzien in eenvoud van beheer
- **Implicatie** (hoe)
  - De core switches ondersteunen MEC
  - De core switches ondersteunen NFV voor het creëren van één virtuele switch

Ontwerpkeuze: De LAN infrastructuur is gebaseerd op een loop-vrij laag-2 ontwerp
- **Rationale** (waarom)
  - Voorzien in hoge beschikbare infrastructuur
- **Implicatie** (hoe)
  - De access switches worden fysiek en redundant gekoppeld met de twee core/distributie switches
  - Deze fysieke verbindingen worden geïmplementeerd als één logische verbinding

LAN infrastructuur fysiek

Ontwerpkeuze: De twee core switches worden geplaatst in een afzonderlijke cabinet

Rationale (waarom)

- Voorzien in hoge beschikbaarheid
- Voorzien in geografische scheiding

Implicatie (hoe)

- De core switches worden geplaatst in de MER, elk in een afzonderlijk cabinet

Ontwerpkeuze: De access-laag bestaat uit meerdere 48-poorts switches geïmplementeerd als één logische switch

Rationale (waarom)

- Voorzien in hoge beschikbaar
- Voorzien in schaalbaarheid
- Voorzien in eenvoud voor beheer
- Besparing van uplinks poorten in acces-laag en distibutie-laag

Implicatie (hoe)

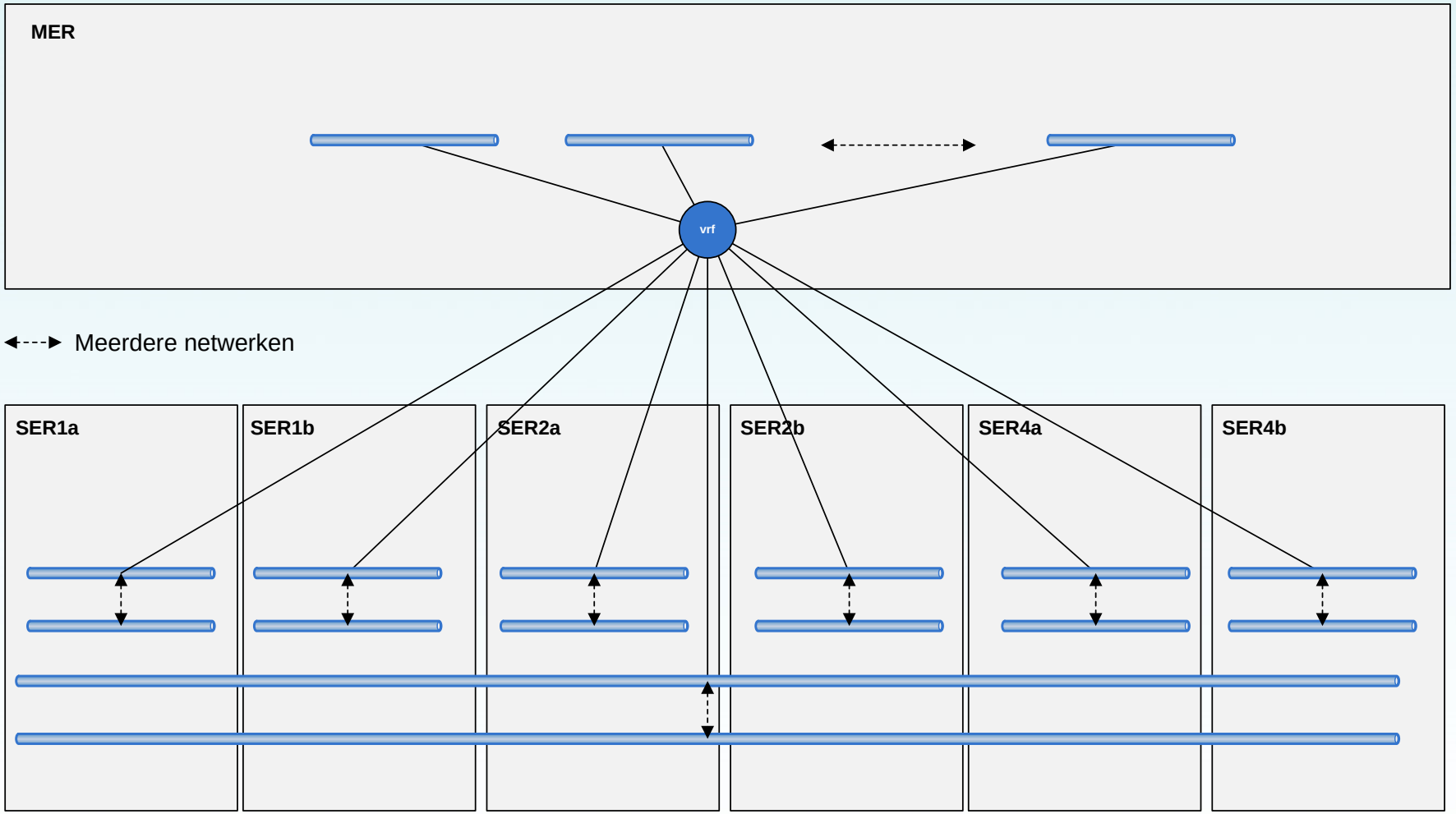
- De access-switches worden geïmplementeerd als één stack (stacking technologie)
- Vanuit een SER zijn slechts twee uplink connecties met de core/distributie-laag

LAN infrastructuur fysiek

Ontwerpkeuze: De core-laag voorziet in SFP+ poorten
- **Rationale** (waarom)
  - Voorzien in 10 Gig koppelvlak voor connectiviteit met de access-laag
  - Voorzien in 1 Gig en 10 Gig koppelvlak voor lokale services
  - Voorzien in flexibiliteit
  - Voorzien in koper en glas koppelvlak
- **Implicatie** (hoe)
  - Koper of glas koppelvlak wordt bepaald door het type SFP

Ontwerpkeuze: De access-laag voorziet in 1 Gig koper poorten en 10 Gig SFP poorten
- **Rationale** (waarom)
  - Voorzien in 1 Gig koppelvlak voor endpoint devices
  - Voorzien in 10 Gig koppelvlak voor uplink poorten
  - Voorzien in backward compatibiliteit met huidige omgeving
- **Implicatie** (hoe)
  - De access switches voorzien in 48 x 1Gig koper poorten en minimaal 2 x 10 Gig SFP poorten

LAN infrastructuur logisch



LAN infrastructuur logisch

Ontwerpkeuze: De core laag bestaat uit twee core switches geïmplementeerd als één logische router

Rationale (waarom)

Voorzien in hoge beschikbaar
Voorzien in schaalbaarheid
Voorzien in eenvoud voor beheer

Implicatie (hoe)

De core switches ondersteunen NFV voor het creëren van één virtuele router

Ontwerpkeuze: De LAN infrastructuur voorziet in logisch gescheiden netwerken backward compatible met de huidige infrastructuur

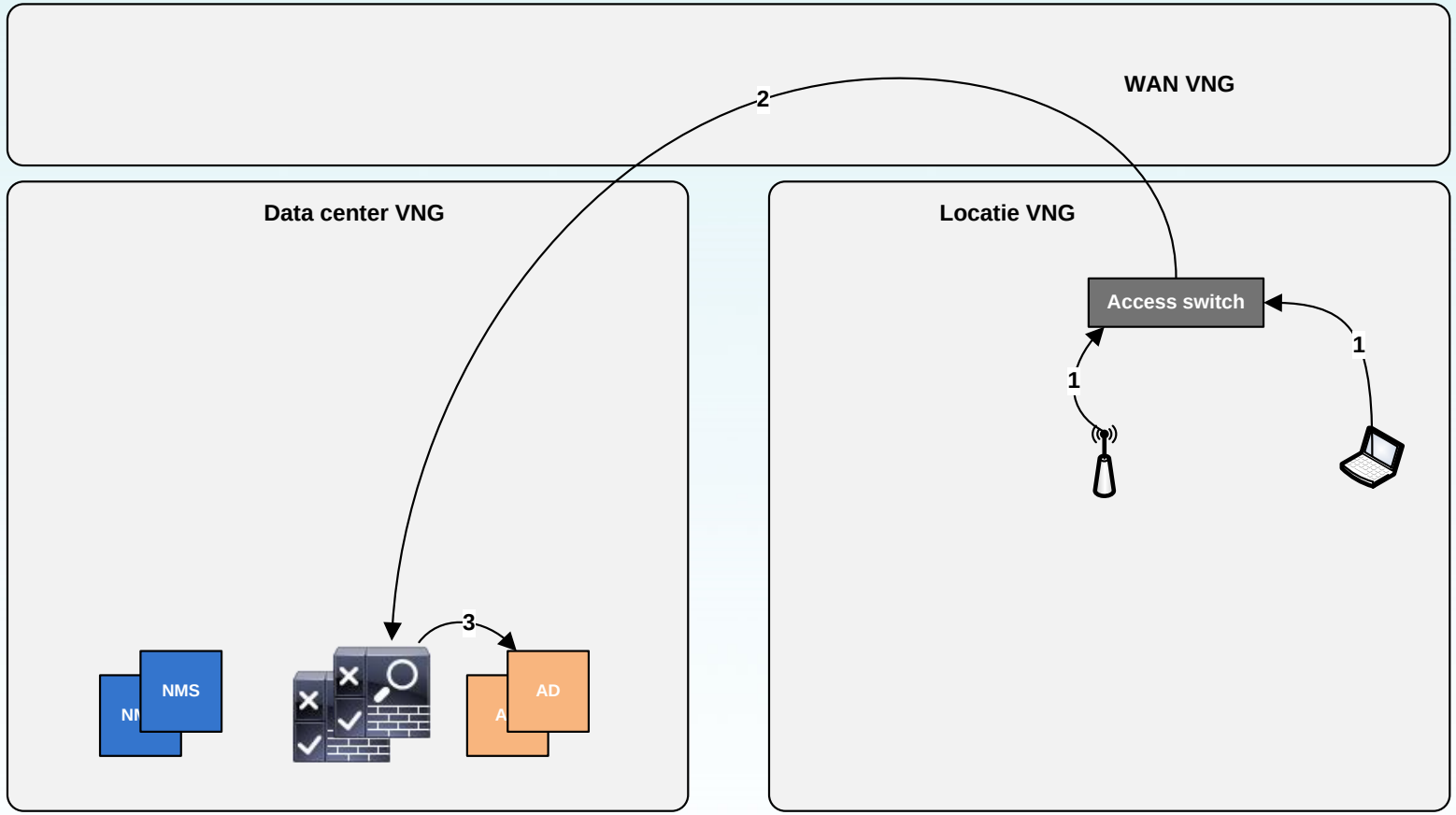
Rationale (waarom)

Voorzien in netwerkzonering
Voorzien in beveiliging van zones
Voorzien in eenvoud van migratie

Implicatie (hoe)

De netwerkzonering is gebaseerd op stretched en lokale VLANs
(stretched over alle MER's en SER's en lokaal per SER en MER)
De beveiliging is gebaseerd op ACL's

Wired architectuur



Wired architectuur

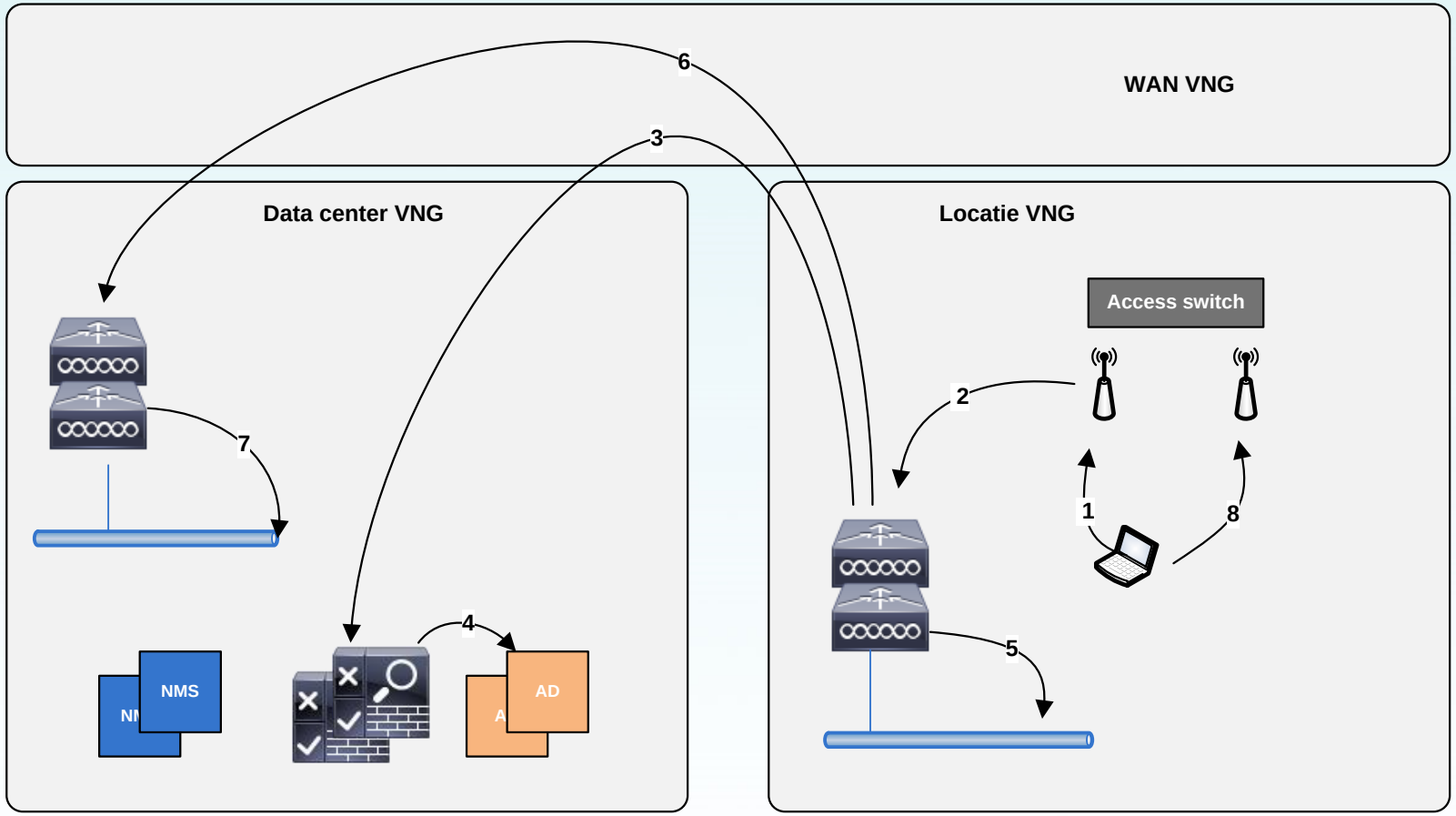
NMS system t.b.v. beheer access switches

1) Wired device wordt gekoppeld met switch

2) Radius request bij centrale NAC service
NAC service doet authenticatie en autorisatie
NAC authentiseert switch voor het koppelen van het device met het netwerk

3) Optioneel: NAC server doet request bij AD voor device/gebruiker authenticatie

Wireless architectuur



Wireless architectuur

NMS system t.b.v. beheer access switches

1) Wireless device heeft radio contact met AP
2) Request via CAPWAP tunnel bij centrale WLAN controller
3) Radius request bij centrale NAC service
   NAC service doet authenticatie en autorisatie
4) Optioneel: NAC server doet request bij AD voor device/gebruiker authenticatie
5) NAC service authentiseert WLAN controller voor het koppelen van het device met het netwerk
6) Gast of BYOD (alleen Internet toegang)
   Verzoek wordt doorgezet naar de anchor WLAN controller
   Anchor WLAN controller bevindt zich in DMZ
7) Anchor WLAN controller koppelt device met DMZ netwerk (lees Internet)
8) Als het wireless device zich in het kantoor verplaatst wordt hij automatisch gekoppeld met een andere AP (roaming)

Wireless architectuur

Ontwerpkeuze: authenticatie en autorisatie van de wireless endpoint devices wordt geregeld door een WLAN service

Rationale (waarom)

- Gecontroleerde en veilige toegang voor de wireless endpoint devices met het netwerk
- Ondersteunen van Internet toegang voor VNG gasten

Implicatie (hoe)

- Specificeren/classificeren van de verschillende wireless netwerken
- Specificeren van SSID per wireless netwerk
- Implementeren van redundante WLAN service
- AP's configureren binnen de WLAN service
- Configureren van de wireless netwerken binnen de WLAN service
- Unmanaged devices krijgen enkel toegang tot Internet (gasten netwerk)

Ontwerpkeuze: De WLAN service wordt lokaal geïmplementeerd binnen de LAN infrastructuur

Rationale (waarom)

- Standaardisatie voor wired en wireless endpoint devices
- Netwerken voor endpoint devices bevinden zich enkel op locatie, en niet in het datacenter

Implicatie (hoe)

- Redundante implementatie van WLAN service in LAN infrastructuur

Wireless architectuur

Ontwerpkeuze: De WLAN anchor service wordt centraal geïmplementeerd binnen de DMZ van het datacenter

Rationale (waarom)

Ondersteunen van Internet toegang voor VNG gasten

Voorzien in logisch gescheiden netwerk voor gasten

Implicatie (hoe)

Redundante implementatie van WLAN anchor service in datacenter

Ontwerpkeuze: Een wireless site survey meting bepaald de infrastructuur van de AP's

Rationale (waarom)

Bepalen van de dekkingsgraad voor WLAN infrastructuur

Bepalen van aantal AP's en van de positie van deze AP's

Netwerk geschikt maken voor voice en video over IP

Implicatie (hoe)

Gebruik maken van de wireless site survey uitgevoerd in november 2019

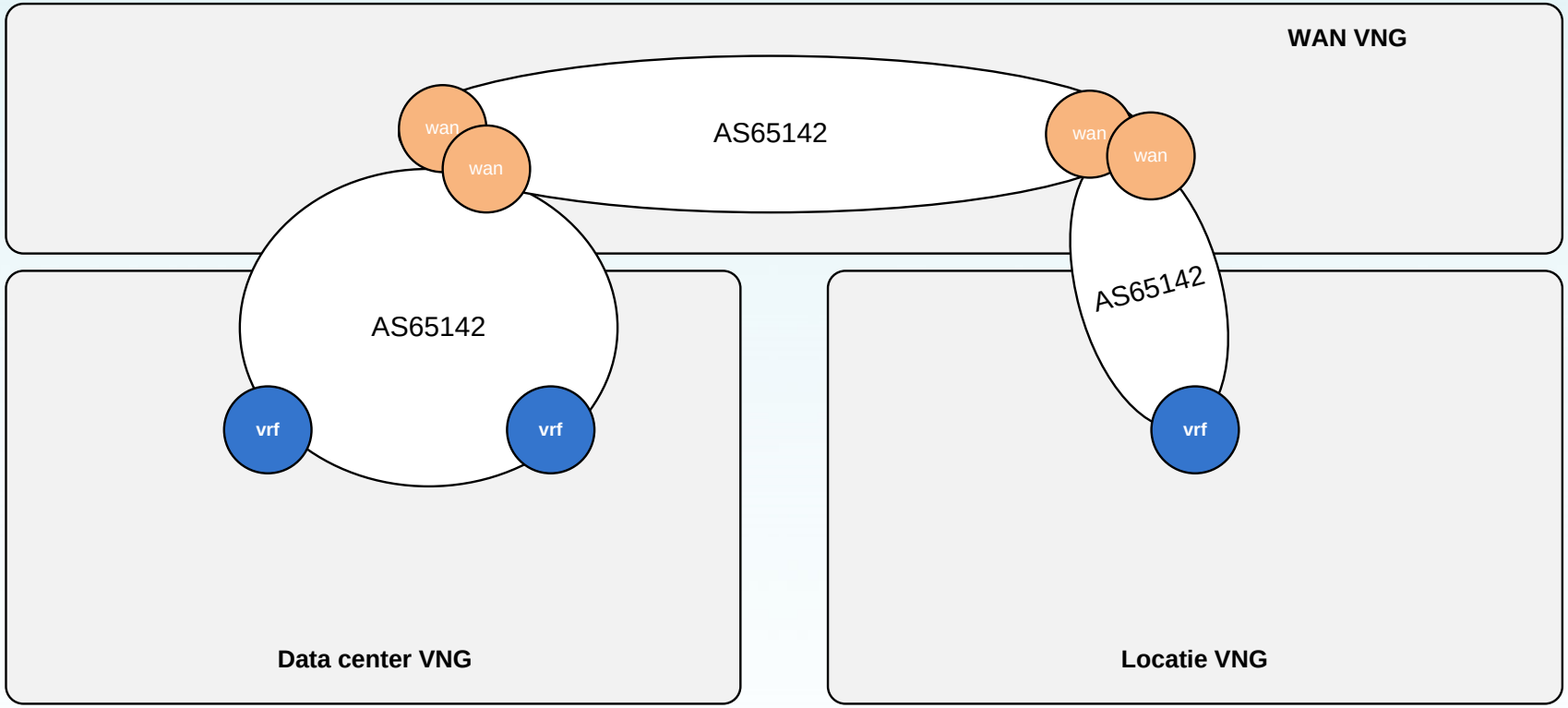
Uitvoeren van een nieuwe meting na uitvoering van de aanpassingen

Rekening houden met voice en video over wifi

Uitvoeren voor zowel de 5GHz band als de 2,4 GHz band

Netwerk services

Routering


WAN VNG
wan
wan
AS65142
wan
wan
AS65142
AS65142
vrf
vrf
vrf
Data center VNG
Locatie VNG

Routering

Ontwerpkeuze: de routering binnen de LAN infrastructuur is gebaseerd op statische routering

Rationale (waarom)

De LAN infrastructuur heeft een statisch karakter

LAN infrastructuur bestaat uit één core router met ‘directly connected’ netwerken

Implicatie (hoe)

Endpoint devices hebben een default route voor de core router

Compute, storage en netwerk devices hebben een default route voor de core router

Ontwerpkeuze: de routering met het WAN is gebaseerd op dynamische routering

Rationale (waarom)

Dynamische failover bij uitval van redundante WAN verbindingen

Hoge beschikbaarheid van connectiviteit met datacenter

Implicatie (hoe)

BGP implementatie op WAN routers en core router

IPAM

Ontwerpkeuze: Handhaven van as-is IP blok toekenning daar waar deze voldoet

Rationale (waarom)

- Voorkomen van IP omnummering
- Backwards compatibiliteit

Implicatie (hoe)

- IP toekenning conform huidig proces

Ontwerpkeuze: Een endpoint device kan dynamisch voorzien worden van een IP adres

Rationale (waarom)

- Eenvoud in configuratie en administratie
- Voorzien in mobiliteit van endpoint devices

Implicatie (hoe)

- Afstemmen welke endpoint devices bestemd zijn voor dynamische IP toekenning
- Inrichten van een DHCP service

Ontwerpkeuze: De compute, storage en netwerk componenten krijgen een fixed IP adres

Rationale (waarom)

- Statisch karakter m.b.t. netwerkconnectiviteit van compute, storage en netwerk devices
- Eenvoud van beheer m.b.t. o.a. DNS en firewall

Implicatie (hoe)

- Afstemmen en registreren binnen IPAM tooling
- Geen DHCP, dynamische DNS en dynamische policies vereist

DHCP

Ontwerpkeuze: T.b.v. dynamische IP uitgifte wordt gebruik gemaakt van een centrale DHCP service

Rationale (waarom)

Dynamisch toekennen van IP adres aan de endpoint devices

Implicatie (hoe)

Operationeel zijn van centrale DHCP service

Core router configureren met DHCP relay functie

QoS

Ontwerpkeuze: QoS binnen de infrastructuur wordt ingericht voor latency gevoelige verkeersstromen en voor de kritische applicaties

Rationale (waarom)

Latency gevoelige verkeersstromen dienen voorrang te krijgen op bulk verkeer

Kritische applicaties dienen een gegarandeerd bandbreedte te krijgen

Implicatie (hoe)

Specificeren/classificeren van de latency gevoelige verkeersstromen (bijvoorbeeld voice)

Specificeren/classificeren van de kritische applicaties

Specificeren/classificeren van de gegarandeerde bandbreedte voor de kritische applicaties

Netwerk componenten worden geconfigureerd met een priority queue (default settings voor QoS)

Latency gevoelige verkeersstromen worden geclassificeerd als EF en geplaatst in de priority queue

Netwerk componenten worden geconfigureerd met één of meerdere queues voor de kritische applicaties

Als uitgangspunt voor de QoS implementatie uitgaan van het huidige QoS ontwerp en de huidige QoS implementatie

Ontwerpkeuze: QoS wordt toegepast voor de control plane van de switches van de LAN infrastructuur

Rationale (waarom)

Beveiliging tegen overbelasting van control plane (DOS aanval)

Implicatie (hoe)

Enkel de voor de control plane van belang zijnde verkeersstromen worden toegelaten tot de control plane

DNS

Ontwerpkeuze: De netwerkcomponenten maken gebruik van de centrale DNS service

- **Rationale** (waarom)
  - Standaardisatie van naamgeving en IP adressering
  - Compute, storage en netwerkcomponenten gebruiken dezelfde naamgeving
- **Implicatie** (hoe)
  - Operationeel zijn van de centrale primaire DNS service
  - Configureren van de DNS service binnen de netwerkcomponenten

NTP

Ontwerpkeuze: De netwerkcomponenten maken gebruik van de centrale NTP service

Rationale (waarom)

Compute, storage en netwerkcomponenten werken met dezelfde tijd (o.a. belangrijk voor analyse logging)

Implicatie (hoe)

Operationeel zijn van de centrale NTP service

Configureren van de NTP service binnen de netwerkcomponenten

Beveiliging

Ontwerpkeuze: De netwerkcomponenten worden geïmplementeerd met hardening conform de CIS benchmark

Rationale (waarom)

Hardening als best practices beveiliging maatregel

Minimaliseren van beveiligingsrisico's. Elke extra service/proces/functie is een risico voor vulnerabilities

Implicatie (hoe)

Alleen de voor het netwerkcomponent van toepassing zijnde service/proces/functie worden geactiveerd

Specificeren van de CIS benchmark per netwerkcomponent

Netwerkcomponent implementeren conform de CIS benchmark

Ontwerpkeuze: AAA voor Inband beheer van de netwerkcomponenten

Rationale (waarom)

Alleen geautoriseerde beheerders krijgen toegang tot de netwerkcomponenten

Implicatie (hoe)

Er dient een centrale AAA service ingeregeld te worden

Netwerkcomponenten dienen te authentiseren bij deze AAA service

Ontwerpkeuze: de netwerkcomponenten worden geplaatst in een afgesloten ruimte alleen toegankelijk voor geautoriseerde personen

Rationale (waarom)

Beveiliging tegen ongeoorloofde fysieke toegang

Implicatie (hoe)

Er dient een toegangscontrole systeem ingeregeld te worden

NAC

Ontwerpkeuze: De infrastructuur is voorbereid op de implementatie van een NAC service

Rationale (waarom)

Voorzien in identiteit beheer en micro-segmentatie voor endpoint devices (managed en unmanaged)

Implicatie (hoe)

De access switches ondersteunen 802.1x, MAB en web authenticatie

T.b.v. de implementatie van de NAC service:

Inventariseren van de type endpoint devices

Specificeren van de beveiliging policies (authenticatie en autorisatie) per type endpoint device


VALID
STAY AHEAD