Advies blauwdruk netwerkontwerp

Blauwdruk netwerkontwerp Afeer

Algemeen

Document informatie

Klant	Afeer
Straat	Romijnweg 17
Postcode	9672 AH
Stad	Winschoten
Document naam	Netwerk blauwdruk advies rapport
Versienummer	V0.1
Classificatie	Voor vertrouwde partijen
Datum	07-01-2025
Auteur	Jeroen Schoolen

INHOUDSOPGAVE

1 Managementsamenvatting

De leverancier zorgt voor het netwerk technische stuk van de omgeving. Hierbij zitten de volgende componenten in scope:

- Wireless LAN (access points)
- LAN (switches, zowel core als access)
- NAC (ClearPass)
- Aruba Central (management en beheer)

Het document beschrijft het nieuwe netwerk van Afeer. Er is gekozen voor een netwerk met producten uit het Aruba Portfolio. Door alle apparatuur op te nemen in het management platform van Aruba, genaamd Aruba Central creëren we een omgeving die met één cloud applicatie te beheren en te monitoren is, ook wel SD-BRANCH genaamd.

Het design is gemaakt met het “security first” principe. Dit betekent dat door de hele lijn er goed is gekeken naar veiligheid van het netwerk. Door de aanschaf van Aruba Clearpass wordt het netwerk naar een “hoger” niveau getild.

Het document wat u momenteel voor u heeft liggen heeft een technische inslag. Vooral de keuze van het opnemen van ClearPass heeft een grote impact voor het uiteindelijke design. Hierbij geven wij onderstaande aanvullend aan waarom dit van belang is voor Afeer. Dit trachten wij op een zo min mogelijke technische manier over te brengen, echter is en blijft dit een complex verhaal.

Wat is Aruba ClearPass en waarom is het belangrijk?

Aruba ClearPass is een oplossing die Afeer helpt om te controleren wie toegang heeft tot het computernetwerken en wat ze daar mogen doen. Het is een essentieel onderdeel van netwerkbeveiliging en helpt Afeer om veilig en efficiënt te werken. Hier zijn enkele redenen waarom het voor Afeer nuttig kan zijn:

Controle over wie er binnenkomt:

Met ClearPass kunnen we precies bepalen wie toegang heeft tot het netwerk. We kunnen verschillende toegangsniveaus instellen voor medewerkers, gasten, en andere gebruikers. Dit helpt Afeer om gevoelige informatie te beschermen en ongeautoriseerde toegang te voorkomen.

Sterke beveiliging:

ClearPass ondersteunt geavanceerde beveiligingsmethoden, zoals wachtwoorden en certificaten, om ervoor te zorgen dat alleen geautoriseerde mensen toegang krijgen tot het netwerk. Dit helpt om Afeer te beschermen tegen hacken en andere beveiligingsrisico's.

Eenvoudige toegang voor gasten:

Als Afeer gasten willen verwelkomen, zoals klanten of consultants, maakt ClearPass het gemakkelijk om hen veilige toegang te geven tot specifieke delen van het netwerk, zonder de kernsystemen in gevaar te brengen. Dit zorgt voor een gastvrije omgeving zonder de beveiliging te compromitteren.

Handhaving van bedrijfsbeleid:

ClearPass helpt Afeer om regels op te stellen voor wat mensen binnen het netwerk mogen doen. We kunnen bijvoorbeeld bepalen welke applicaties ze kunnen gebruiken of welke websites ze kunnen bezoeken. Dit helpt Afeer om de beleidsregels te handhaven en risico's te minimaliseren.

Identificatie van apparaten:

ClearPass kan herkennen welke apparaten verbinding maken met het netwerk, of het nu computers, smartphones, of tablets zijn. Hierdoor kan Afeer snel reageren op ongebruikelijke apparaten of verdachte activiteiten.

Betere compliance:

Voor bedrijven die moeten voldoen aan bepaalde regels en voorschriften (zoals GDPR, BIO, NEN of ISO), kan ClearPass Afeer helpen bij het voldoen aan deze eisen door te zorgen voor een veilige en gecontroleerde omgeving. We kunnen ook rapporten genereren om de compliance te laten zien.

Door Aruba ClearPass te gebruiken, kunnen we de netwerkbeveiliging verbeteren, ongeautoriseerde toegang voorkomen, en een veiligere werkomgeving creëren. Het is een investering in de veiligheid en efficiëntie, wat uiteindelijk bijdraagt aan de bedrijfscontinuïteit en reputatie.

Op basis van de bovenstaande uitleg en de aanvullende technische uitleg verderop in dit document zijn wij er van overtuigd jullie een zo goed mogelijk beeld te geven van hoe wij dit advies hebben opgebouwd.

2 Doelstelling

Door het schrijven van een blauwdruk voor het nieuw te ontwerpen datanetwerk komt er eenheid in de netwerk inrichting. Hierdoor wordt het beheer vereenvoudigd en komt er meer controle over het netwerk, waardoor er een hogere mate van betrouwbaarheid is van het netwerk.

Gevraagd is om een netwerk te ontwerpen waar zowel het kantoor datanetwerk als het productie netwerk samen komen in één switch omgeving. Ook dient er rekening gehouden te worden met de applicaties in de cloud.

In dit document zijn de specificaties opgenomen van het gewenste netwerkdesign. Er wordt een advies neergelegd welke apparatuur er in welke omgeving ingezet dient te worden. Daarnaast wordt er dieper ingegaan op technische invulling van het netwerk, zoals VLAN's en SSID's en netwerkbeveiliging.

2.1 Scope van het rapport

In het rapport zijn de onderstaande onderwerpen opgenomen:

- WAN verbindingen
- SD-BRANCH met SDWAN
- Aruba Central
- Azure
- Apparatuur
- Lokale netwerk
- Security en beheer

3 AFEER-locaties

Afeer beschikt over meerdere locaties in de provincie Groningen van uiteenlopende grootte. De locaties hebben we in orde van grootte van de werkplekken opgedeeld in drietal klassen. Door de locaties op te delen in drie klassen kunnen we een passend ontwerp neerleggen die aansluit bij het aantal gebruikers.

Er is voor gekozen om twee verschillende klassen te definiëren, namelijk:

- Klasse A, 75 en meer werkplekken;
- Klasse B, 10 en meer (tot klasse A) op basis van werkplekken en hardware selectie.

*Werkplekken is een combinatie van de aantallen welke aangeleverd zijn door Afeer.
Voorbeeld: MFP + Vergaderruimtes + kantoren + werkplekken.

Locatie	Adres	Plaats	Werkplekken	Klasse
Romijnweg	Romijnweg 17	Winschoten	+- 110	A
Hogebrug	Winschoter Hogebrug 1	Blijham	+- 90	A
Werklab Pekela	H. Hindersstraat 54	Oude Pekela	+- 15	B
Werklab Vlagtwedde	Spetsebrugweg 1B	Vlagtwedde	+- 10	B
Bellingwolde	Hoofdweg 256A	Bellingwolde	+- 10	B

4 WAN verbindingen

Per locatie zullen er internetverbindingen benodigd zijn. Geadviseerd wordt om symetrische verbindingen met voldoende bandbreedte aan te schaffen. Voor de klasse A locaties wordt geadviseerd minimaal 200Mbps, voor de klasse B is 100Mbps voldoende.

Waarneer er LAN verkeer tussen de locaties noodzakelijk is of naar het Azure private cloud wordt geadviseerd om SDWAN mee te nemen in het design.

5 Aruba SD-BRANCH

Software gedefinieerde branch (SD-Branch) is een technologische verschuiving naar oplossingen die flexibel, open en in de cloud geïntegreerd zijn. SD-Branch bevat een component genaamd SD-WAN die een veilig, serviceprovider onafhankelijk netwerk levert met prestaties op Enterprise niveau via ongelijksoortige wide-area network (WAN) -technologieën.

Echter, hoewel SD-WAN een echt IT-probleem oplost, lost het slechts een deel van het probleem op waarmee organisaties worden geconfronteerd: gedistribueerde locaties.

Hier komt SD-Branch om de hoek kijken. Hierbij komen de LAN-, WLAN- component en SD-WAN component samen. SD-Branch = SD-WAN + SD-LAN

SD-Branch bestaat uit een aantal componenten waarvan de configuratie in dit document wordt beschreven. Onderdelen zijn:

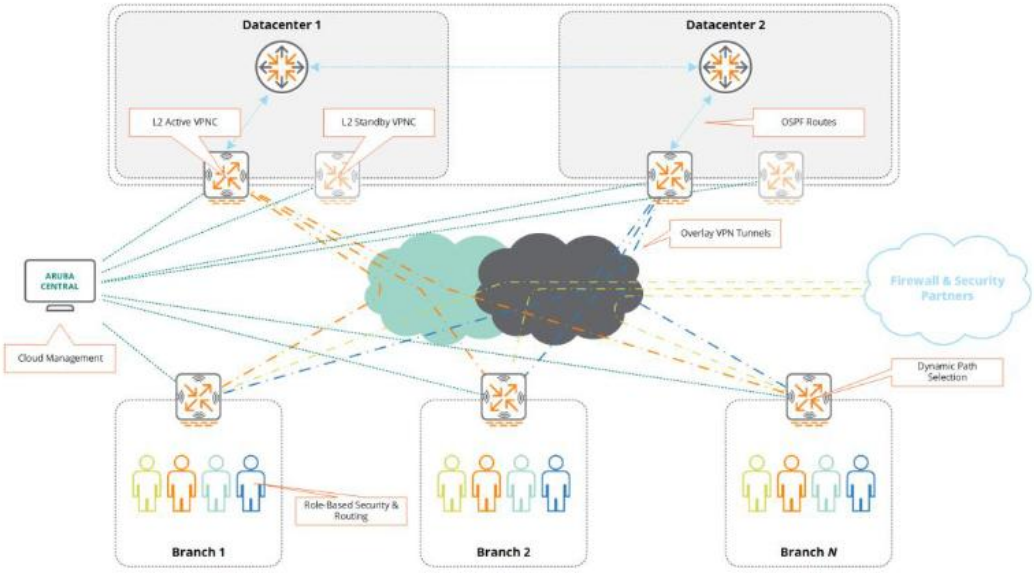
- VPNC (VPN Concentrator)
- BGW of wel Branch Gateway
- Switch
- Access Point(s)
- ClearPass

Voor SDWAN bestaat de configuratie globaal uit twee lagen. Het underlay netwerk en het overlay netwerk.

Het underlay netwerk is de basis waarover de tunnels, het overlay netwerk, opgebouwd zullen worden. IP-adressen, voor bijvoorbeeld de internetverbinding, vallen bijvoorbeeld in het underlay netwerk. Het definiëren van de tunnels valt dan weer in de tweede laag. Het overlay netwerk.

5.1 Aruba Central

Aruba Central is het platform dat gebruikt wordt om de SD-Branch omgeving te beheren en te monitoren. De volledige SD-Branch omgeving zal worden opgenomen in Aruba Central. In Aruba Central wordt de configuratie uitgevoerd en gepushed naar de verschillende in apparaten.



Bovenstaande afbeelding geeft de positie weer van Aruba Central in een SD-Branch oplossing. Aruba Central wordt gezien als het cloud managementsysteem van de SD-Branch omgeving. De groene stippellijnen illustreren de communicatie van Aruba Central naar alle componenten. Onderdeel van SD-Branch is SD-WAN.

6 Azure

Benodigde applicaties en diensten zijn gepositioneerd in Azure. Onderstaand zijn de diensten neergezet welke belang zijn voor het netwerk.

6.1 Connectiviteit

Middels een site2site verbinding vanaf een VPN-Concentrator kan er connectie worden gemaakt vanuit het LAN naar Azure. In het meest ideale scenario wordt de VPN-Concentrator niet op een locatie gepositioneerd maar in Azure private cloud. Middels BRANCH-MESH technologie kan locatie naar locatie verkeer worden gerouteerd rechtstreeks naar de locaties, daarmee kan op een slimme manier omgegaan worden met het dataverbruik in Azure.

6.2 Servers

In Azure dienen een aantal centrale servers te worden opgenomen:

- DHCP-server t.b.v. dynamisch toewijzen IP-adressen;
- DNS-server t.b.v. name resolving.

6.3 Netwerkbeveiliging

Om authenticatie voor de netwerkapparatuur op centraal niveau in te richten en beheren adviseren we een TACACS+ of RADIUS server, zoals Aruba Clearpass.
Voor centrale logging adviseren we een Syslog server op te nemen in het datacenter, mits ervoor gekozen wordt om de switches op te nemen in Aruba Central. Dit wordt beschreven in hoofdstuk 11.

6.3.1 TACACS+ Server

TACACS+ wordt gebruikt voor authenticatie / autorisatie / accounting (AAA), hiermee wordt op een centrale plek de toegang beheerd voor de netwerkcomponenten. Geadviseerd wordt persoonlijke accounts uit te geven met betrekking tot vastleggen van de gebeurtenissen op het netwerk. Voor Afeer zal Aruba Clearpass deze rol vervullen.

6.3.2 Syslog server

Geadviseerd wordt om logging van de netwerkcomponenten te sturen naar een centrale Syslog server in het datacenter. Hiermee wordt op een centrale plek alle logging verzameld van de netwerkcomponenten. Wanneer er gekozen wordt om de switches centraal te beheren in Aruba Central is een SYSLOG server in het datacenter niet benodigd.

7 Kitlijst

Azure DC		
	HPE Aruba Networking ClearPass Access License 1K Concurrent Endpoints E-LTU	1
	Aruba 5Y FC SW CP NL AC 1K CE E-L SVC [for JZ402AAE]	1
	HPE Aruba Networking Virtual Gateway 500Mbps 5-year Subscription E-STU	1
	HPE Aruba Networking ClearPass NAC Cx000V VM-Based Appliance License E-LTU	1
	Aruba 5Y FC SW CP Cx000V VMAppl E-L SVC [for JZ399AAE]	1

Bellingwolde - Bellingwolde		
	HPE Aruba Networking 9004 (RW) 4-Port GbE RJ45 2K Clients - 32 APs Gateway	1
	Aruba 5Y FC NBD Exch HW 9004 Gtwy SVC [for R1B21A]	1
	HPE Aruba Networking PC-AC-EC 250V/10A 1.8m C13 to CEE7/7 (EU) AC Power Cord	1
	HPE Aruba Networking 90/70xx Central Gateway Foundation 5-year Subscription E-STU	1
	HPE Aruba Networking 9004-MNT-19 9004 Series 19-inch Rack Mount Kit	1
	HPE Aruba Networking Central AP Foundation 5-year Subscription E-STU	1
	HPE Aruba Networking Central Switch Class-1 Foundation 5-year Subscription E-STU	1
	HPE Aruba Networking CX 6200F 12G Class4 PoE 2G/2SFP+ 139W Switch	1
	Aruba 5Y FC NBD Exch HW 6200F 12G SVC [for R8Q72A]	1
	HPE Aruba Networking AP-505 (RW) Dual Radio 2x2 802.11ax Internal Antennas Unified Campus AP	1
	Aruba 5Y FC NBD Exch HW AP-505 SVC [for R2H28A]	1
	HPE Aruba Networking AP-MNT-D Campus AP mount bracket kit (individual) type D: solid surface	1

Hogebrug - Blijham		
	HPE Aruba Networking Central AP Foundation 5-year Subscription E-STU	22
	HPE Aruba Networking Central Switch Class-2 Foundation 5-year Subscription E-STU	9
	HPE Aruba Networking AP-505 (RW) Dual Radio 2x2 802.11ax Internal Antennas Unified Campus AP	22
	Aruba 5Y FC NBD Exch HW AP-505 SVC [for R2H28A]	22
	HPE Aruba Networking AP-MNT-MP10-D Campus AP mount bracket kit (10-pack) type D: solid surface	2
	HPE Aruba Networking AP-MNT-D Campus AP mount bracket kit (individual) type D: solid surface	2
	HPE Aruba Networking CX 6200F 48G Class4 PoE 4SFP+ 370W Switch	5

	Aruba 5Y FC NBD Exch HW 6200F 48G CL4 4SFP+ 370W SVC [for JL727B]	5
	FLEXOPTICS 10G SFP+ LC LR 10km SMF C-class	5
	HPE Aruba Networking CX 6200F 48G Class4 PoE 4SFP+ 370W Switch	1
	Aruba 5Y FC NBD Exch HW 6200F 48G CL4 4SFP+ 370W SVC [for JL727B]	1
	HPE Aruba Networking 9004 (RW) 4-Port GbE RJ45 2K Clients - 32 APs Gateway	2
	Aruba 5Y FC NBD Exch HW 9004 Gtwy SVC [for R1B21A]	2
	HPE Aruba Networking PC-AC-EC 250V/10A 1.8m C13 to CEE7/7 (EU) AC Power Cord	2
	HPE Aruba Networking 90/70xx Central Gateway Foundation 5-year Subscription E-STU	2
	HPE Aruba Networking 9004-MNT-19 9004 Series 19-inch Rack Mount Kit	1
	HPE Aruba Networking CX 6200M 48G Class4 PoE 4SFP+ Switch	1
	Aruba 5Y FC NBD Exch HW 6200M 48G PoE SVC [for R8Q70A]	1
	HPE Aruba Networking X372 54VDC 680W 100-240VAC Power Supply	2
	FLEXOPTICS 10G SFP+ LC LR 10km SMF C-class	2
	HPE Aruba Networking CX 6200M 24G Class4 PoE 4SFP+ Switch	1
	Aruba 5Y FC NBD Exch HW 6200M 24G PoE SVC [for R8Q68A]	1
	HPE Aruba Networking X372 54VDC 680W 100-240VAC Power Supply	2
	FLEXOPTICS 10G SFP+ LC LR 10km SMF C-class	2
	HPE Aruba Networking CX 6200M 24G Class4 PoE 4SFP+ Switch	1
	Aruba 5Y FC NBD Exch HW 6200M 24G PoE SVC [for R8Q68A]	1
	HPE Aruba Networking X372 54VDC 680W 100-240VAC Power Supply	2
	FLEXOPTICS 10G SFP+ LC LR 10km SMF C-class	1
	HPE Aruba Networking 10G SFP+ to SFP+ 1m Direct Attach Copper Cable	7

Romijnweg - Winschoten		
	HPE Aruba Networking 9004 (RW) 4-Port GbE RJ45 2K Clients - 32 APs Gateway	2
	Aruba 5Y FC NBD Exch HW 9004 Gtwy SVC [for R1B21A]	2
	HPE Aruba Networking PC-AC-EC 250V/10A 1.8m C13 to CEE7/7 (EU) AC Power Cord	2
	HPE Aruba Networking 90/70xx Central Gateway Foundation 5-year Subscription E-STU	2
	HPE Aruba Networking 9004-MNT-19 9004 Series 19-inch Rack Mount Kit	1
	HPE Aruba Networking Central AP Foundation 5-year Subscription E-STU	27
	HPE Aruba Networking Central Switch Class-2 Foundation 5-year Subscription E-STU	6
	HPE Aruba Networking CX 6200M 48G Class4 PoE 4SFP+ Switch	2
	Aruba 5Y FC NBD Exch HW 6200M 48G PoE SVC [for R8Q70A]	2
	HPE Aruba Networking X372 54VDC 680W 100-240VAC Power Supply	4
	FLEXOPTICS 10G SFP+ LC LR 10km SMF C-class	4
	HPE Aruba Networking AP-505 (RW) Dual Radio 2x2 802.11ax Internal Antennas Unified Campus AP	27

	Aruba 5Y FC NBD Exch HW AP-505 SVC [for R2H28A]	27
	HPE Aruba Networking AP-MNT-MP10-D Campus AP mount bracket kit (10-pack) type D: solid surface	2
	HPE Aruba Networking AP-MNT-D Campus AP mount bracket kit (individual) type D: solid surface	7
	HPE Aruba Networking CX 6200F 48G Class4 PoE 4SFP+ 370W Switch	4
	Aruba 5Y FC NBD Exch HW 6200F 48G CL4 4SFP+ 370W SVC [for JL727B]	4
	FLEXOPTICS 10G SFP+ LC LR 10km SMF C-class	4
	HPE Aruba Networking 10G SFP+ to SFP+ 1m Direct Attach Copper Cable	6

Werklab Pekela - Oude Pekela		
	HPE Aruba Networking 9004 (RW) 4-Port GbE RJ45 2K Clients - 32 APs Gateway	1
	Aruba 5Y FC NBD Exch HW 9004 Gtwy SVC [for R1B21A]	1
	HPE Aruba Networking PC-AC-EC 250V/10A 1.8m C13 to CEE7/7 (EU) AC Power Cord	1
	HPE Aruba Networking 90/70xx Central Gateway Foundation 5-year Subscription E-STU	1
	HPE Aruba Networking 9004-MNT-19 9004 Series 19-inch Rack Mount Kit	1
	HPE Aruba Networking Central AP Foundation 5-year Subscription E-STU	2
	HPE Aruba Networking Central Switch Class-2 Foundation 5-year Subscription E-STU	1
	HPE Aruba Networking CX 6200F 48G Class4 PoE 4SFP+ 370W Switch	1
	Aruba 5Y FC NBD Exch HW 6200F 48G CL4 4SFP+ 370W SVC [for JL727B]	1
	HPE Aruba Networking AP-505 (RW) Dual Radio 2x2 802.11ax Internal Antennas Unified Campus AP	2
	Aruba 5Y FC NBD Exch HW AP-505 SVC [for R2H28A]	2
	HPE Aruba Networking AP-MNT-D Campus AP mount bracket kit (individual) type D: solid surface	2

Werklab Vlagtwedde - Vlagtwedde		
	HPE Aruba Networking 9004 (RW) 4-Port GbE RJ45 2K Clients - 32 APs Gateway	1
	Aruba 5Y FC NBD Exch HW 9004 Gtwy SVC [for R1B21A]	1
	HPE Aruba Networking PC-AC-EC 250V/10A 1.8m C13 to CEE7/7 (EU) AC Power Cord	1
	HPE Aruba Networking 90/70xx Central Gateway Foundation 5-year Subscription E-STU	1
	HPE Aruba Networking 9004-MNT-19 9004 Series 19-inch Rack Mount Kit	1
	HPE Aruba Networking Central AP Foundation 5-year Subscription E-STU	2
	HPE Aruba Networking Central Switch Class-2 Foundation 5-year Subscription E-STU	1
	HPE Aruba Networking CX 6200F 48G Class4 PoE 4SFP+ 370W Switch	1
	Aruba 5Y FC NBD Exch HW 6200F 48G CL4 4SFP+ 370W SVC [for JL727B]	1
	HPE Aruba Networking AP-505 (RW) Dual Radio 2x2 802.11ax Internal Antennas Unified Campus AP	2

	Aruba 5Y FC NBD Exch HW AP-505 SVC [for R2H28A]	2
	HPE Aruba Networking AP-MNT-D Campus AP mount bracket kit (individual) type D: solid surface	2

Artikelen (Stelpost Extra AP's)		**#**
	HPE Aruba Networking Central AP Foundation 5-year Subscription E-STU	23
	HPE Aruba Networking AP-505 (RW) Dual Radio 2x2 802.11ax Internal Antennas Unified Campus AP	23
	Aruba 5Y FC NBD Exch HW AP-505 SVC [for R2H28A]	23
	HPE Aruba Networking AP-MNT-MP10-D Campus AP mount bracket kit (10-pack) type D: solid surface	2
	HPE Aruba Networking AP-MNT-D Campus AP mount bracket kit (individual) type D: solid surface	3

8 Locatie netwerk

In dit hoofdstuk beschrijven we de uitgangspunten voor het datanetwerk in elke klasse. In hoofdstuk 3 beschrijven we de opdeling van de twee klassen (A/B). Elke klasse heeft zijn specifieke wensen / eisen die past bij de omvang van de locatie. Per locatieklasse beschrijven we onderstaande onderwerpen:

- Redundantie;
- Verbindingen;
- LAN Netwerkapparatuur;
- WLAN Netwerkapparatuur;
- Dekkingsgraad WLAN;
- Netwerkbeveiliging;
- Noodstroomvoorziening.

8.1 Klasse A

Een klasse A locatie heeft meer dan 75 werkplekken.

8.1.1 Redundantie

Overall redundantie is geen vereiste, maar een advies. Geadviseerd wordt om de primaire WAN-verbinding te voorzien van een back-up verbinding. De switchomgeving wordt waar mogelijk dubbel uitgevoerd. Waarbij er gekeken wordt naar het aantal benodigde poorten. Bij meer dan 24 werkplekpoorten wordt er geadviseerd twee 24 poort switches in een stack te plaatsen i.p.v. een enkele 48 poort switch.

Verbindingen tussen switches en tussen verschillende SER's worden dubbel en met glasvezel uitgevoerd. Het draadloze netwerk kent geen extra redundantie.

8.1.2 WAN verbinding

Geadviseerd wordt om naast de primaire SD-WAN een secundaire verbinding als back-up te hebben.

In het geval van een enkele SD-WAN verbinding, waarbij een back-up verbinding is voorzien in hetzelfde apparaat wordt geadviseerd om dubbel aan te sluiten richting de switchomgeving, verdeeld over verschillende switches.

8.1.3 LAN Netwerkapparatuur

8.1.3.1 Branch gateway / VPNC

Om SDWAN te faciliteren is er een branch gateway (BGW) en een VPN-Concentrator (VPNC) benodigd. Een BGW dient als terminatie van de clients en het opzetten van de tunnels richting de VPNC, waarbij de VPNC alle tunnels aan elkaar verbindt en er een SDWAN topologie ontstaat. De BGW is niet alleen essentieel voor SDWAN maar dient tevens als locatie firewall.
Met het concept kleurloze poorten zal de BGW tevens dienen als terminatiepunt voor de clients en access points. Per client zal er een rol worden toegewezen waarin de firewall regels voor het type clients wordt toegekend, ook wel microsegmentatie genoemd. Hiermee wordt de veiligheid en controle in het netwerk aanzienlijk vergroot.

Voor een klasse A is er gekozen voor de Aruba 9004 Branch Gateway alsmede voor de VPN-Concentrator. Dit type heeft voldoende kracht om bovenstaande functionaliteiten af te handelen.

- 4x 1GE ports
- Supported devices 128
- Max. clients 2000
- Dimensions: 43.7 mm (H) x 294.8 mm (W) x 201.05mm (D)

8.1.3.2 Switches

Door routing en firewalling op de BGW af te handelen is er geen extra krachtige Core switch met additionele routing functionaliteiten vereist.

Voor een locatie klasse A hebben we gekozen voor Aruba 6200F switches. Altijd in een gestackte opstelling wanneer er meer dan één switch wordt geïnstalleerd. De access-poorten zijn van het type koper 10/100/1000 Mbit/s. De uplinkpoorten zijn van het type SFP+ 10Gbit/s en worden uitgerust met Aruba 10G SFP+ LC SR Netwerk tranciever modules.

De Aruba CX 6200 Switch-serie is een familie van stackable switches, ideaal voor vestigingen en campussen, maar ook voor het MKB.

De switch kan ingezet worden als standaard switch, maar heeft de mogelijkheid voor Dynamic Segmentation, ook in een later stadium. Om de netwerkbeveiliging voor IoT en mobiliteit op de werkplek te verbeteren, splitst Aruba Dynamic Segmentation automatisch het verkeer, zowel over bekabelde als draadloze netwerken.

In een klasse A is gekozen voor de ARUBA 6200F 24G CLASS4 POE 4SFP+ 370W SWITCH (JL725A/B).

- 24x ports 10/100/1000BaseT PoE+ ports supporting up to 30W per port
- 4x 1/10G SFP+ ports
- Internal (fixed) power supply (500W), fixed fans
- Up to 370W of Class 4 PoE
- Dimensions: (H) 4.39 cm x (W) 44.2 cm x (D) 32.7 cm (1.73" x 17.4" x 12.9")
- Weight: 4.9 kg

De stacking-mogelijkheden zorgen er voor dat meerdere switch-componenten één logische entiteit vormen. Dit stacken gebeurt bij de 6200F op basis van VSF.

Binnen de access nodes zullen geen protocollen als Spanning Tree gebruikt worden voor redundantie, wel ter voorkoming van ongewenste lussen in het netwerk door patch fouten. Daarnaast zullen protocollen als Loop-protection ingezet worden ter voorkoming van ongewenste lussen in het netwerk. De ontsluiting naar de code nodes zal plaats vinden op basis van twee keer 10Gbit/s samengevoegd tot één bundel middels het Link aggregation protocol LACP (IEEE802.3ad).

De 6200F heeft de mogelijkheid tot geavanceerde routing, zoals dynamische routing protocollen. Bij Afeer wordt de 6200F ook als “top of rack” switch ingezet. De “top of rack” switch voorziet de routeringen tussen de lokale netwerken en het WAN.

8.1.4 WLAN Netwerkapparatuur

Als access point worden verschillende type access points geadviseerd. Dit zijn de Aruba 616 en 635 access points. Beide modellen zijn WiFi6E access points.

Voor in de ruimtes waar er minder clients zullen connecteren op het wireless netwerk zoals in de kamers/appartementen van de bewoners, in de gangen, liften, trappenhuizen, technische ruimtes en de kleinere kantoren wordt het Aruba 615 access point geadviseerd. Het Aruba 615 access point is met zijn 2x2

MU-MIMO(Multi-User Multiple Input Multiple Output) omni antennes op zowel de 2.4GHz als de 5GHz of 6GHz uitermate geschikt om deze ruimtes te bedienen. De Aruba 615 kan op twee banden tegelijk actief zijn. Dit betekent dat uit de drie beschikbare banden een keus uit twee gemaakt moet worden.

In ruimtes waar meer clients samenkomen zoals de grote kantoortuinen, restaurants en de grotere recreatieruimtes wordt het Aruba 635 access point geadviseerd. Het Aruba 635 access point is een krachtiger tri-band access point dan het Aruba 615 access point en heeft op de 2x2 MU-MIMO omni antennes op alle drie de banden. Hierdoor kan deze meer clients tegelijkertijd bedienen.

ARUBA 610 SERIES

ARUBA 630 SERIES

8.1.5 Dekkingsgraad WLAN

Voor een Klasse A netwerk geld een volledige dekkingsgraad binnen de gebouwen.

Geadviseerd wordt een dekkingsgraad met een minimale signaalsterkte van -67dBm en een signaal/ruisverhouding van 30dB.

8.1.6 Netwerkbeveiliging

Geadviseerd wordt om gebruik te maken van een aantal standaard veiligheidsfuncties:

- BPDU-GUARD
- LOOP PROTECT
- PORT SECURITY
- DHCP SNOOPING

Deze veiligheidsfuncties BPDU-GUARD en LOOP PROTECT dragen bij om lussen in het netwerk te voorkomen. Om onder andere wildgroei van unmanaged switches tegen te gaan wordt met behulp van PORT SECURITY de poorten geblokkeerd zodra er meer dan twee netwerkcomponenten op een werkplekpoort wordt aangesloten. DCHP SNOOPING wordt gebruikt om DHCP-server verkeer wat aangeboden wordt op de werkplekpoorten te blokkeren.

8.1.7 Dynamic Segmentation

Het concept ‘Kleurloze poorten’ (zie hoofdstuk 9) is een Aruba Clearpass Policy Manager een vereiste. De user based tunnels (UBT) termineren op de lokale Branch Gateway, waar het een policy door de ClearPass krijgt toegewezen. De Branch Gateway faciliteert tevens SDWAN en firewalling. Extra hardware op locatie is niet nodig.

8.1.8 Noodstroomvoorziening

Geadviseerd wordt om alle netwerkapparatuur in de patchkasten achter een noodstroomvoorziening (UPS) met ByPass te plaatsen. De ByPass functie zorgt ervoor dat onderhoud aan de UPS, zoals vervangen van de accu’s tijdens bedrijf kan worden uitgevoerd, zonder dat de achterliggende apparatuur hiervoor uit moet. Spanningspieken en spanningsdippen worden door de UPS opgevangen en bij stroomuitval blijft het netwerk voor een X aantal minuten functioneren. Minimaal 30 minuten is hierin het advies.

Wanneer er een noodstroom aggregaat aanwezig is op locatie mag de tijd korter zijn dan 30 minuten. Daarmee wordt de capaciteit ook kleiner van de UPS.

8.2 Klasse B

Een klasse B locatie heeft minder dan 75 werkplekken.

8.2.1 Redundantie

Redundantie is niet van toepassing op een klasse B locatie.

8.2.2 Verbinding

Naast de primaire SD-WAN verbinding (glas / koper) adviseren we een back-up 4G verbinding.

8.2.3 LAN Netwerkapparatuur

8.2.3.1 Branch gateway

Om SDWAN te faciliteren is er een branch gateway (BGW) benodigd. De BGW is niet alleen essentieel voor SDWAN maar dient tevens als locatie firewall. Met kleurloze poorten zal de BGW tevens dienen als terminatiepunt voor de clients en access points. Per client zal er een rol worden toegewezen waarin de firewall regels voor het type clients wordt toegekend, ook wel microsegmentatie genoemd. Hiermee wordt de veiligheid en controle in het netwerk aanzienlijk vergroot.

Voor een klasse A is er gekozen voor de Aruba 9004 (LTE) Branch Gateway. Dit type heeft voldoende kracht om bovenstaande functionaliteiten af te handelen. Een VPN-Concentrator is niet van toepassing op een klasse B

- 4x 1GE ports
- Supported devices 128
- Max. clients 2000
- Dimensions: 43.7 mm (H) x 294.8 mm (W) x 201.05mm (D)

8.2.3.2 Switches

Bij een klasse A locatie is gekozen voor de Aruba 6200F series. De 6200F series hebben de mogelijkheid voor een extra securityfeature, namelijk Dynamic Segmentation. Met Dynamic Segmentation wordt het verkeer op de poort gesplitst en getunneld naar een gateway.

De Aruba 6200F series heeft in het portfolio geen switches met minder dan 24 poorten. Voor de klasse B locaties zal de keus voor een switch afhangen van de wens op extra security in de vorm van Dynamic Segmentation.

De Aruba 6100 series beschikt in het portfolio over switches met minder dan 24 poorten, maar heeft als limitatie dat Dynamic Segmentation niet wordt ondersteund.

In een klasse B, waarbij Dynamic Segmentation (extra security) gewenst is, wordt er gekozen voor de ARUBA 6200F 24G CLASS4 POE 4SFP+ 370W SWITCH (JL725A/B). Zie paragraaf 7.1.3.2 voor verdere specificaties.

8.2.4 WLAN Netwerkapparatuur

Als access point worden verschillende type access points geadviseerd. Dit zijn de Aruba 616 en 635 access points. Beide modellen zijn WiFi6E access points.

Voor in de ruimtes waar er minder clients zullen connecteren op het wireless netwerk zoals in de kamers/appartementen van de bewoners, in de gangen, liften, trappenhuizen, technische ruimtes en de kleinere kantoren wordt het Aruba 615 access point geadviseerd. Het Aruba 615 access point is met zijn 2x2 MU-MIMO(Multi-User Multiple Input Multiple Output) omni antennes op zowel de 2.4GHz als de 5GHz of 6GHz uitermate geschikt om deze ruimtes te bedienen. De Aruba 615 kan op twee banden tegelijk actief zijn. Dit betekent dat uit de drie beschikbare banden een keus uit twee gemaakt moet worden.

In ruimtes waar meer clients samenkomen zoals de grote kantoortuinen, restaurants en de grotere recreatieruimtes wordt het Aruba 635 access point geadviseerd. Het Aruba 635 access point is een krachtiger tri-band access point dan het Aruba 615 access point en heeft op de 2x2 MU-MIMO omni antennes op alle drie de banden. Hierdoor kan deze meer clients tegelijkertijd bedienen.

ARUBA 610 SERIES

ARUBA 630 SERIES

8.2.5 Dekkingsgraad WLAN

Voor een klasse B netwerk geldt geen volledige dekkingsgraad binnen de gebouwen.

Geadviseerd wordt een dekkingsgraad met een minimale signaalsterkte van -67dBm en een signaal/ruisverhouding van 30dB.

8.2.6 Netwerkbeveiliging

Geadviseerd wordt om gebruik te maken van een aantal standaard veiligheidsfuncties:

- BPDU-GUARD
- LOOP PROTECT
- PORT SECURITY
- DHCP SNOOPING

Deze veiligheidsfuncties BPDU-GUARD en LOOP PROTECT dragen bij om lussen in het netwerk te voorkomen. Om onder andere wildgroei van unmanaged switches tegen te gaan wordt met behulp van PORT SECURITY de poorten geblokkeerd zodra er meer dan twee netwerkcomponenten op een werkplekpoort wordt aangesloten. DCHP SNOOPING wordt gebruikt om DHCP-server verkeer wat aangeboden wordt op de werkplekpoorten te blokkeren.

8.2.7 Dynamic Segmentation

Middels het concept ‘Kleurloze poorten’ (zie hoofdstuk 9) is een Aruba ClearPass Policy Manager een vereiste. De user based tunnels (UBT) termineren op de lokale Branch Gateway, waar het een policy door de ClearPass krijgt toegewezen. De Branch Gateway faciliteert tevens SDWAN en firewalling. Extra hardware op locatie is niet nodig.

8.2.8 Noodstroomvoorziening

Noodstroomvoorzieningen zijn optioneel.

9 Netwerkbeveiliging / NAC

Naast de implementatie van standaard security gerelateerde mechanismes, zoals IP DHCP SNOOPING, BPDU-GUARD, PORT SECURITY en LOOP PROTECT op het lokale netwerk adviseren we sterk om de beveiliging van het netwerk naar een hoger niveau te brengen.

Het nieuwe netwerk gaat worden gebruikt door kantoorautomatisering, facilitaire diensten, IoT en gasten. Met al deze verschillende disciplines op het netwerk is een hoge mate van beveiliging gewenst. Hiermee krijg je een hogere betrouwbaarheid van het netwerk.

Door het concept ‘Kleurloze poorten’ te implementeren in het netwerk kan er dynamisch omgegaan worden met allerlei verschillende netwerkapparatuur zonder veiligheid te verliezen met het oog op BIO richtlijnen.

9.1 Kleurloze poorten

Het gebruik van netwerken wordt steeds veelzijdiger en de diversiteit van apparaten op het netwerk is flink toegenomen. Beveiliging zal hier een belangrijk aspect moeten zijn. Sommige devices zullen netjes 802.1X ondersteunen, sommige helaas niet. Een deel hiervan zullen zelfs headless IoT devices zijn.

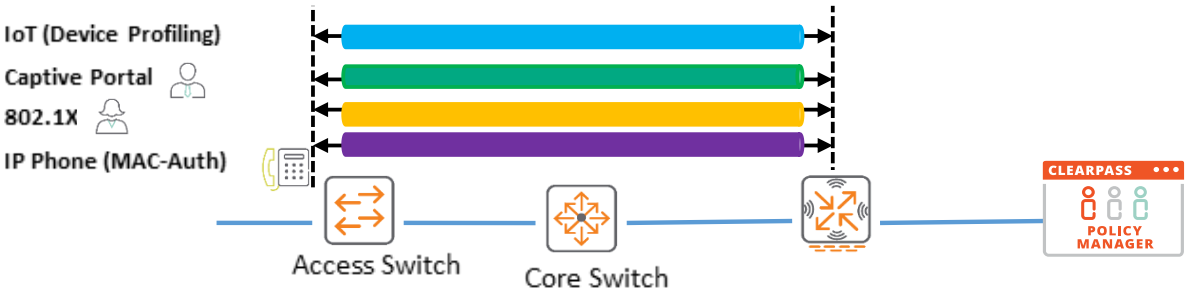
Als beheerders, verantwoordelijk voor de veiligheid van de infrastructuur, willen we niet zoals traditioneel gebeurde, per apparaat categorie een vlan introduceren met in de kast een stuk papier met daarop met verschillende kleuren aangegeven welke poort voor welke toepassing is. Beter is het als poorten kleurloos zijn en het netwerk bepaald welke apparatuur bij elkaar hoort.

Het grootste effect / voordeel van kleurloze poorten is dat we geen access poorten voor VLAN's statisch hoeven te configureren.

Binnen netwerken was vroeger het concept dat de poorten fysiek een "kleur" kregen op de switch, zodat specifiek beleid aan die poort kon worden toegewezen. Specifieke apparaten kregen een “kleur” toegewezen en konden alleen op de overeenkomstige poorten worden aangesloten.

Door kleurloze poorten te gebruiken, worden de operationele cycli van IT aanzienlijk verkort, wat leidt tot een efficiënte planning voor de eerste implementatie of voortdurende configuratiewijzigingen die toekomstige toevoegingen, verhuizingen of wijzigingen mogelijk maken.

9.1.1 User-Based Tunneling



Veel apparaten die netwerktoegang nodig hebben, Power over Ethernet (PoE) en non-POE zoals beveiligingscamera's, printers, betaalkaartlezers en medische apparaten, hebben geen ingebouwde beveiligingssoftware zoals een desktop- of laptopcomputer. Deze apparaten kunnen een risico vormen voor netwerken met een gebrek aan beveiliging. Met rol gebaseerde tunneling, User-Based Tunneling, kunnen deze apparaten worden geverifieerd met ClearPass en kan het verkeer van deze apparaten worden getunneld naar de Aruba (Branch) Gateway. Met behulp van de geavanceerde firewall en beleidsmogelijkheden in de Aruba gateway kunnen er vervolgens bepaalde spelregels opgesteld worden wat een apparaat wel of niet mag.

Op deze manier kan een veilige toegang voor IoT-apparaten binnen het Aruba Wired Intelligent Edge-netwerk gerealiseerd worden.
Ieder apparaat krijgt een “User Role” ofwel rol toegewezen. Deze rol bevat regels die bepalen wat het apparaat wel en niet mag.

De voordelen van het toewijzen van "rollen" aan gebruikers en / of apparaten zijn bekend binnen de draadloze wereld van Aruba. Deze is eenvoudig overgenomen naar de bedrade switchpoort. Net als bij Aruba Wireless, is er nu de mogelijkheid om de configuratielast te vereenvoudigen, door beleid te groeperen in een "rol" waarnaar kan worden verwezen door veel apparaat- of gebruikerstypen. Bovendien kan met ClearPass context worden toegevoegd (tijd van de dag, type machine, apparaat profilering) bij het beslissen of een gebruiker / apparaat wordt toegestaan op het netwerk en welke toegangsrechten worden verleend of geweigerd.

Een rol zal op zijn minst bepalen welke VLAN moet worden toegewezen en of het verkeer lokaal wordt geschakeld of terug naar de gateway wordt getunneld. Optioneel kan een rol ook een beleid (ACL / QOS), her-verificatietimers en een captive portal-omleiding toewijzen.

Apparaat profilering vindt in dit geval plaats op basis van MAC OUI van het device en bepaalde DHCP parameters.

9.1.2 Infrastructuur

Om dit te kunnen realiseren zijn een aantal componenten nodig. Zo moet de access laag worden voorzien van switches die User Based Tunneling ondersteunen en dient er een (branch) gateway in het netwerk aanwezig te zijn die de tunnels termineren.

Aan software is er een ClearPass Policy Manager (CPPM) nodig om het beleid van Afeer te vertalen naar een stuk programmering van het netwerk. Samen met de Mobility Controllers wordt dit het punt waar de spelregels worden geprogrammeerd.

User Based Tunneling wordt ondersteund op o.a. de 2930F, 2930M, 5400R, 3810 en voor AOS-CX switches vanaf de 6200F switches. Van de 6100 en 6200 series die bij Afeer zijn geadviseerd, beschikt alleen de 6200 series over compatibiliteit aan deze set van functies.

10 MER en SER-ruimtes

In dit hoofdstuk bespreken we de gewenste inrichting van de MER en SER-ruimtes.

10.1 Patchruimtes

De patchruimtes dienen stofvrij en opgeruimd te zijn. De ruimtes dienen ten allen tijde goed toegankelijk te zijn. De patchruimtes zijn niet bedoeld als opslagruimtes voor overig materiaal of voor middelen van de schoonmaker.

Het advies is om de ruimtes aan een aantal standaard eisen te laten voldoen. Waar de ruimtes niet voldoen zal gekeken moeten worden wat er nodig is om ze aan de standaard eisen te voldoen.

- 19inch patchkasten moeten minimaal 80 cm breed en 80 cm diep zijn voor klasse A netwerken, voor klasse B mag de minimale diepte afwijken i.v.m. eventuele wandkasten;
- Patchkasten en patchruimtes zijn voorzien van unieke codering;
- Voor elke patchpaneel van 24 werkplekpoorten dient een rangeerpaneel geplaatst te worden;
- Glasvezelpatchpanelen dienen zo hoog mogelijk in de kast gemonteerd te worden en te worden voorzien van een rangeerpaneel;
- Patchkabel begeleiders aan de spijlen van de patchkasten;
- Patchkasten moeten afsluitbaar zijn;
- Er dient een spanningsslof met overspanningsbeveiliging achter een gezekerde stroomgroep aanwezig te zijn in de patchkast;
- Optioneel: twee spanningssloffen met overspanningsbeveiliging achter twee gezekerde stroomgroepen;
- Advies voor gaasdeuren i.p.v. glazen deuren in de patchkasten, zodat koude lucht de patchkast in kan.

10.2 Klimaatbeheersing

Het juiste klimaat in de SER en MER-ruimtes is in het belang van de levensduur van de apparatuur. Onderstaand het advies omtrent klimaatbeheersing.

- Temperatuur in de ruimte tussen de 20 en 25 graden;
- De patchkasten beschikken over mechanische afzuiging;
- Vochtigheidsgraad tussen de 10 en 90% om condensvorming te voorkomen.

10.3 Kleurcodering patchbekabeling

Om een eenduidig beeld te creëren in de patchkasten wordt geadviseerd om verschillende kleuren patchkabels te gebruiken. Hiermee kan onderscheid gemaakt tussen werkplekken en essentiële verbindingen van het lokale netwerk.

Er is gekozen voor het concept “Kleurloze poorten”, daarmee is elke switchpoort voor elk netwerkcomponent te gebruiken. Aan de hand van User Based Tunneling (UBT) worden policy ’s gepushed en komt een component in het juiste segment. Alle access poorten worden hiermee voorzien van dezelfde patchkabel kleur.

Toepassing	**Kleur (zonder kleurloze poorten)**	**Kleur (met kleurloze poorten)**	**Opmerking**
Werkplek, telefonie	Grijs	Grijs	Standaard werkplekken incl. telefonie
Routers, switches, uplinks	Rood	Rood	Alle essentiële netwerkverbindingen voor het LAN
Access points	Geel	Grijs	
Automation	Paars	Grijs	

11 Globale inrichting netwerk

Globaal gemaakte afspraken over de inrichting van het netwerk is essentieel voor een eenduidig netwerk. Door te standaardiseren is de kans op het maken van fouten kleiner en wordt de beheerlast verlaagd. De uiteindelijk inrichting zal worden vastgelegd in een Low Level Design (LLD). Onderstaand is een globaal overzicht gecreëerd hoe het eruit kan zien.

11.1 Naamconventies

Om eenduidigheid te creëren in de benaming van de IT-apparatuur adviseren we een standaard aan te houden. De label moet kort zijn maar duidelijk aangeven om welk type apparaat het gaat. Dubbele namen zijn niet toegestaan.

[Klantnaam]-[locatiebenaming]-[apparaat type]-[volgnummer]

11.2 VLANs

We adviseren om op elke locatie de standaard VLANs aan te maken. Ook wanneer VLANs niet worden gebruikt. De VLAN ID's dienen op elke locatie hetzelfde te zijn om verwarring te voorkomen.

Voorbeeld:

VLAN ID	Naam	Beschrijving
1	Default	Standaard VLAN, niet gebruikt
10	Data	Bedrade clients
20	Data WLAN	Draadloze clients zoals laptops
30	Telefonie	Telefoons
40	Beveiliging	GBS-componenten
42	CCTV	Camera netwerk
50	Shared	Printers, NAS, etc.
80	Gasten	Bedrade gasttoegang
90	Gasten WLAN	Draadloze gastentoegang
120	Management	Management netwerkapparatuur
122	Management AP	Management access points
250	Transit WAN	Transitie VLAN tussen Afeer en ISP SD-Branch DC
251	Transit WWW	Transitie VLAN tussen Afeer en ISP SD-Branch WWW

11.3 SSID's

In overleg zullen de SSID's afgestemd moeten worden. Met het concept 'kleurloze poorten' is door de aanwezigheid van een ClearPass Policy Manager het aantal SSID te beperken naar het type authenticatie dat gewenst is voor het SSID.

Geadviseerd wordt om maximaal drie SSID's per band uit te zenden.

Voor voice over WLAN SSID's zal gekeken moeten worden met welk type clients gebeld gaat worden en hierop een passend SSID in te richten die voldoet aan de eisen van het toestel.

11.4 IP-plan

Het advies is om een "Class A private" IP reeks te reserveren waarin meerdere netwerken kunnen worden uitgedeeld. Om een duidelijke link te leggen tussen het IP-adres en VLAN ID adviseren we deze op te nemen in het IP-adres.

Het transitienetwerk wat op elke vestiging wordt aangemaakt om van-en-naar te kunnen routeren naar ISP zal als een /29 worden gedefinieerd.

Voorbeeld met locatienummer 11 en VLAN ID 10:
10.locatienummer.vlanid.hosts (10.11.10.x)

Voorbeeld:

VLAN ID	Naam	IP-reeks
1	Default	-
10	Data	10.x.10.0/24
20	Data WLAN	10.x.20.0/24
30	Telefonie	10.x.30.0/24
40	Beveiliging	10.x.40.0/24
42	CCTV	10.x.42.0/24
50	Shared	10.x.50.0/24
80	Gasten	10.x.80.0/24
90	Gasten WLAN	10.x.90.0/24
120	Management	10.x.120.0/24
122	Management AP	10.x.122.0/24
250	Transit ISP WAN	10.x.250.0/29
251	Transit ISP WWW	10.x.251.0/29

11.5 Access List (ACL)

In basis routeert de branch gateway alle netwerken waarin een interface is gedefinieerd. Om ervoor te zorgen dat niet alle clients in verschillende netwerken met elkaar kunnen communiceren adviseren wij access-lists (ACL) te configureren op de interfaces. Met behulp van ACL's kunnen we regels opstellen welke netwerken met elkaar mogen communiceren.

Met het concept 'kleurloze poorten' worden er geen ACL's meer geprogrammeerd op de interface maar op een centrale plek, namelijk de ClearPass Policy Manager. Het gebruik van de ClearPass Policy Manager verlaagd de beheerlast aanzienlijk door niet meer elke Core switch individueel te moeten configureren. De kans op fouten zal eveneens afnemen.

11.6 DHCP / DNS / NTP

Geadviseerd wordt om gebruik te maken van centrale DHCP-server(s) en DNS. Om ervoor te zorgen dat de switches dezelfde tijd hebben adviseren we voor alle netwerkcomponenten dezelfde NTP-server te gebruiken.

11.7 Spanning-tree

Het gebruik van spanning-tree voorkomt ongewenste lussen in het netwerk. Geadviseerd wordt om de standaard RSTP spanning-tree variant te gebruiken.

11.8 Quality of Service (QoS)

Goede inrichting van QoS is op een gezamenlijk netwerk een must. Met QoS kan bepaald worden welk type verkeer voorrang verleend moet worden op het netwerk. Juiste QoS inrichting is met name erg belangrijk wanneer het erg druk is op het netwerk en het belangrijke verkeer eerder behandeld moet worden dan het onbelangrijk verkeer. Hierdoor is de kans kleiner dat belangrijk verkeer niet verloren gaat, denk hierbij aan telefonie dataverkeer.

Op het lokale netwerk adviseren we de standaard DSCP-waardes (Laag3 QoS) te honoreren en als "trust" te markeren.

Van belang is dat netwerkclients die belangrijk verkeer willen sturen een hoge DSCP QoS waarde meestuurt met zijn datapakketten, zodat het verkeer op de juiste manier wordt afgehandeld in het netwerk. Als clients geen DSCP-waarde meestuurt maar wel aangemerkt dient te worden als belangrijk verkeer, zal er onderzocht moeten worden hoe QoS kan worden toegepast.

Om QoS te garanderen zal over de hele keten QoS ingericht moeten worden. Met ISP zal moeten worden afgestemd hoe QoS zich in het SD-WAN en VPN-netwerk gedraagt.

12 Netwerkbeheer en monitoring

Het netwerk is in een aantal facetten op te delen, namelijk: Het bedrade netwerk, draadloze netwerk en door het concept ‘Kleurloze poorten’ komt Network Access Control (NAC) erbij. Om het netwerk te kunnen monitoren en beheren zijn een aantal opties mogelijk.

12.1 SDWAN

Het SDWAN wordt beheerd middels Aruba Central. Aruba Central is de “orchestrator” voor het bouwen en beheren van de SDWAN tunnels, waardoor inter-locatie verkeer mogelijk wordt gemaakt.

12.2 Draadloos

De draadloze omgeving zal worden beheerd en gemonitord met Aruba Central. Wijzigingen dienen doorgevoerd te worden in Aruba Central. Lokale configuratie is niet mogelijk.

12.3 Bedraad

Het bedrade netwerk wordt beheerd en gemonitord door Aruba Central. Voor elke switch die gemonitord / beheerd gaat worden door Aruba Central zal een licentie moeten worden aangeschaft.

De switches zullen dan verbinding opbouwen naar Aruba Central en alleen vanuit Aruba Central te beheren zijn.

12.4 Network Access Control

Als er wordt gekozen voor het concept ‘kleurloze poorten’ zullen de rollen op de branch gateways worden beheerd en gemonitord in Aruba Central. In de Clearpass Policy Manger wordt op een centrale plek de regels voor het netwerk beheerd.

12.5 Samenvatting

Met Aruba Central is een volledig beheerbare omgeving te creëren voor zowel het bedrade en draadloos netwerk. Waarbij de draadloos omgeving altijd in Aruba Central beheerd moet worden staat de keus voor de switchomgeving vrij. Een groot voordeel om alles in Aruba Central op te nemen en te beheren is dat alle netwerkapparatuur op een centrale plek staat opgevoerd (SPOG). Doordat alle netwerkcomponenten zijn opgenomen in Central is het volledig datapad van een locatie inzichtelijk te krijgen. Op basis van AI kan Aruba Central mogelijke storingen vroegtijdig detecteren.