NETTVERKSDOKUMENTASJON FOR BÅNSULL AS

Teknisk dokumentasjon og innkjøp

Innholdsfortegnelse

Daniel

1. Innledning

1.1 Hovedformål

Hovedmålet med denne dokumentasjonen er å beskrive Bånsull AS sitt nettverksoppsett og å identifisere de nødvendige ressursene for innkjøp og implementering av dette nettverket. Formålet er å gi en grundig forståelse av bedriftens infrastruktur, samt å veilede gjennom nødvendige steg for å etablere og vedlikeholde det optimale nettverksmiljøet for organisasjonens behov.

Bånsull AS er et firma som driver med salg av ullvarer til bedrifter og sluttbrukere. De har et kontor og en butikk. Dessuten skal de ha mulighet for å ekspandere firmaet på en enkel måte om det blir behov for det.

1.2 Sikkerhetsrammeverk

Bånsull AS må sikre at deres nettverksinfrastruktur er beskyttet mot potensielle trusler og samsvarer med relevante sikkerhetsstandarder. Dette sikkerhetsrammeverket er designet for å adressere nøkkelfaktorene i sikkerhet, basert på NSM Grunnprinsipper, og GDPR-krav.

1.2.1 Nettverkssikkerhet

Vi ønsker implementering av en robust brannmur for å filtrere inngående og utgående trafikk, samt bruk av VLAN-segmentering for å isolere og beskytte sensitive nettverksområder. Dessuten setter vi opp regelbasert tilgangskontroll for å begrense tilgangen til nettverksressurser basert på brukerens rolle og ansvar.[1]

1.2.2 Brukere og Rettighetsstyring

Grunnlaget for en rollebasert tilgangskontroll er en sentralisert brukeradministrasjon via Active Directory, med definerte brukergrupper og rettighetsgrupper. For et sikkert nettverk vil vi ha implementering av sterk passord-policy, som krever lange passord fordi alle brukere benytter MFA. Alle brukere får multifaktor autentisering (MFA) for å styrke tilgangskontrollen til kritiske systemer og ressurser.[2]

1.2.3 Data- og Informasjonssikkerhet

For å sikre konfidensialitet og integritet av data under overføring, vil vi etablere en sikker Virtual Private Network (VPN)-infrastruktur for eksterne tilkoblinger, med fokus på ende-til-ende kryptering.[3] Dessuten vil det være regelmessig sikkerhetskopiering av viktige

---

[1] Se NSM Grunnprinsipper for IKT-sikkerhet 2.0 punkt 2.5.1

[2] Se NSM Grunnprinsipper for IKT-sikkerhet 2.0 punkt 2.6

[3] Se NSM Grunnprinsipper for IKT-sikkerhet 2.0 punkt 2.4.2

Daniel

forretningsdata og oppbevart på en sikker lokasjon. Om personopplysninger skulle gå tapt vil det bli lagd en rapport rundt sikkerhetsbruddet som blir sendt til Datatilsynet innen 72 timer i samsvar med GDPR-krav.[4]

1.2.4 Endepunktssikkerhet

Brukerne på nettverket skal ha oppdatert antivirus- og antimalware-løsninger for å detektere og hindre skadelig programvare. Dersom maskinen ikke kan følge den standarden, vil den bli satt i karantene/'not compliant'. I tillegg til implementering av en policy for sikkerhetsoppdateringer og patching av alle systemer og applikasjoner for å lukke kjente sårbarheter. [5]

1.2.5 Overvåking

Kontinuerlig overvåkning og logging av nettverkstrafikk er også viktig for å identifisere og respondere på potensielle sikkerhetshendelser. [6]

1.2.5 Opplæring og Bevisstgjøring

For at ansatte skal øke bevisstheten om sikkerhetsrisikoer og beste praksis bør det gjennomføres regelmessig sikkerhetsopplæring og skal etableres en responsplan for håndtering av sikkerhetshendelser. Dette inkluderer prosedyrer for raskt å isolere og begrense et sikkerhetsbrudd.[7]

[4] Art. 33 GDPR – Notification of a personal data breach to the supervisory authority
[5] Se NSM Grunnprinsipper for IKT-sikkerhet 2.0 punkt 2.4
[6] Se NSM Grunnprinsipper for IKT-sikkerhet 2.0 punkt 3.2
[7] Se NSM Grunnprinsipper for IKT-sikkerhet 2.0 punkt 4.1

2 Standard oppsett

En standard på nettverk som skal kunne dekke flere forskjellige behov, er å benytte klasse A-nettverk, slik at bedriften har mulighet til å utvide om behovet melder seg.
I dette nettverket blir da 2. oktett lokasjon, og 3. oktett VLAN.

Vi ønsker også gode navn på nettverksutstyret vårt som gjør det enkelt å kjenne igjen og finne feil på. Det er basert på denne malen: [lokasjon]-[utstyr]-[nummer]. Et eksempel på dette er MOS-RUT-01 for en ruter i Moss nummer 01.

Dessuten ønsker vi oss en løsning for forskjellige lokasjoner. Lokasjonene her skal ha en enkel forkortelse som skal brukes på utstyr, og en lokasjons-id for IP-adressen. Eks: Switch 5 i butikken har adresse: 10.2.10.25.

Navn	**Lokasjons-id**	**Forkortelse**
1-Bånsull Kontorer	1	KON
2-Bånsull Butikk	2	BUT

2.1 Utstyr og maskiner

2.1.1 Kontor

På kontoret implementerer vi en brannmur direkte fra internett for å styrke nettverkssikkerheten og overvåke potensielle trusler fra enheter og brukere. Denne brannmuren er tilkoblet en switch for å gi økt kapasitet. I denne switchen knytter vi til et access point og -kontroller for administrasjon av tilkoblede access points. Videre tilkobler vi serveren, printeren, og eventuelle enheter som krever kablet tilgang for å sikre effektiv kommunikasjon.

2.1.2 Butikk

Andre lokasjoner skal ha liknende oppsett; en brannmur med en AP, printer og eventuelle andre kablede tilganger.

3 Budsjett

3.1 Budsjett for 1-Bånsull Kontorer: Nettverk

Alt utstyr er hentet fra Dustin, med unntak av brannmur.

1-Bånsull KON: Nettverkskostnader over 3 år						
Enhet	Enhetsnavn	Enhetspris (Eks. MVA)		Antall	Total	
Brannmur	Palo Alto Networks PA-440	kr	14 627,00	1	kr	14 627,00
Brannmur Bundle	PA-440, Professional Subscription Bundle (Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security), 5 years (60 months) term	kr	13 185,00	1	kr	13 185,00
Brannmur Support	PA-440, Partner enabled premium support, 5 years (60 months), term, renewal.	kr	28 107,00	1	kr	28 107,00
Switch	Cisco CBS250 24G 4SFP PoE 100W Smart Switch 24G 4SFP PoE	kr	3 799,00	1	kr	3 799,00
AP-kontroller	Ubiquiti UniFi Cloud Key Gen2 Plus	kr	2 179,00	1	kr	2 179,00
Access Point	Ubiquiti UniFi U6 Pro Access Point	kr	1 719,00	2	kr	3 438,00
Server	Supermicro SuperServer 5018A-MLTN4 Atom C2550	kr	5 995,00	1	kr	5 995,00
Printer	HP Color LaserJet Pro M282nw A4 MFP	kr	3 639,00	1	kr	3 639,00
Ethernet-0.5m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	72,00	5	kr	360,00
Ethernet-1m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	114,00	10	kr	1 140,00
Ethernet-2m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	125,00	10	kr	1 250,00
Ethernet-5m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	153,00	5	kr	765,00
Ethernet-10m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	219,00	2	kr	438,00
Ethernet-20m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	419,00	2	kr	838,00
			Total		**kr**	**79 760,00**
			Avskrivning over tre år:		**kr**	**26 586,67**

3.1 Budsjett for 1-Bånsull Kontorer: Pult

Alt utstyr er hentet fra Dustin, med unntak av Laptop, fra Lenovo

1-Bånsull KON: Stasjonskostnader over 3 år						
Enhet	Enhetsnavn	Enhetspris		Antall	Total ($)	
	Laptop med dock					
PC	ThinkPad X13 Gen 4 (13" Intel)	kr	13 191,72	9	kr	118 725,48
Dock	Thinkpad Hybrid USB-C Dock	kr	1 999,00	9	kr	17 991,00
PC-stand	R1 Justerbart Mobilt Stativ Romgrå	kr	595,00	9	kr	5 355,00
	Stasjonær					
Stasjonær PC	Ryzen 7 32GB 1000GB SSD	kr	7 999,00	1	kr	7 999,00
	Annet					
Skjerm	CU34V5CW Curved 34" 3440 x 1440 21:9 VA 100Hz	kr	3 899,00	10	kr	38 990,00
Tastatur og mus	Ergo K860 For Business Logi Bolt Nordisk Tastatur	kr	2 099,00	10	kr	20 990,00
Musematte	QcK 3XL Musematte	kr	649,00	10	kr	6 490,00
Headset	Evolve2 65 MS (incl. Stand)	kr	2 399,00	10	kr	23 990,00
Webkamera	C920S HD Pro	kr	999,00	10	kr	9 990,00
Office 365	Microsoft 365 Business Standard (5 år)	kr	9 750,00	10	kr	97 500,00
			Total:		**kr**	**348 020,48**
			Avskrivning over tre år:		**kr**	**116 006,83**

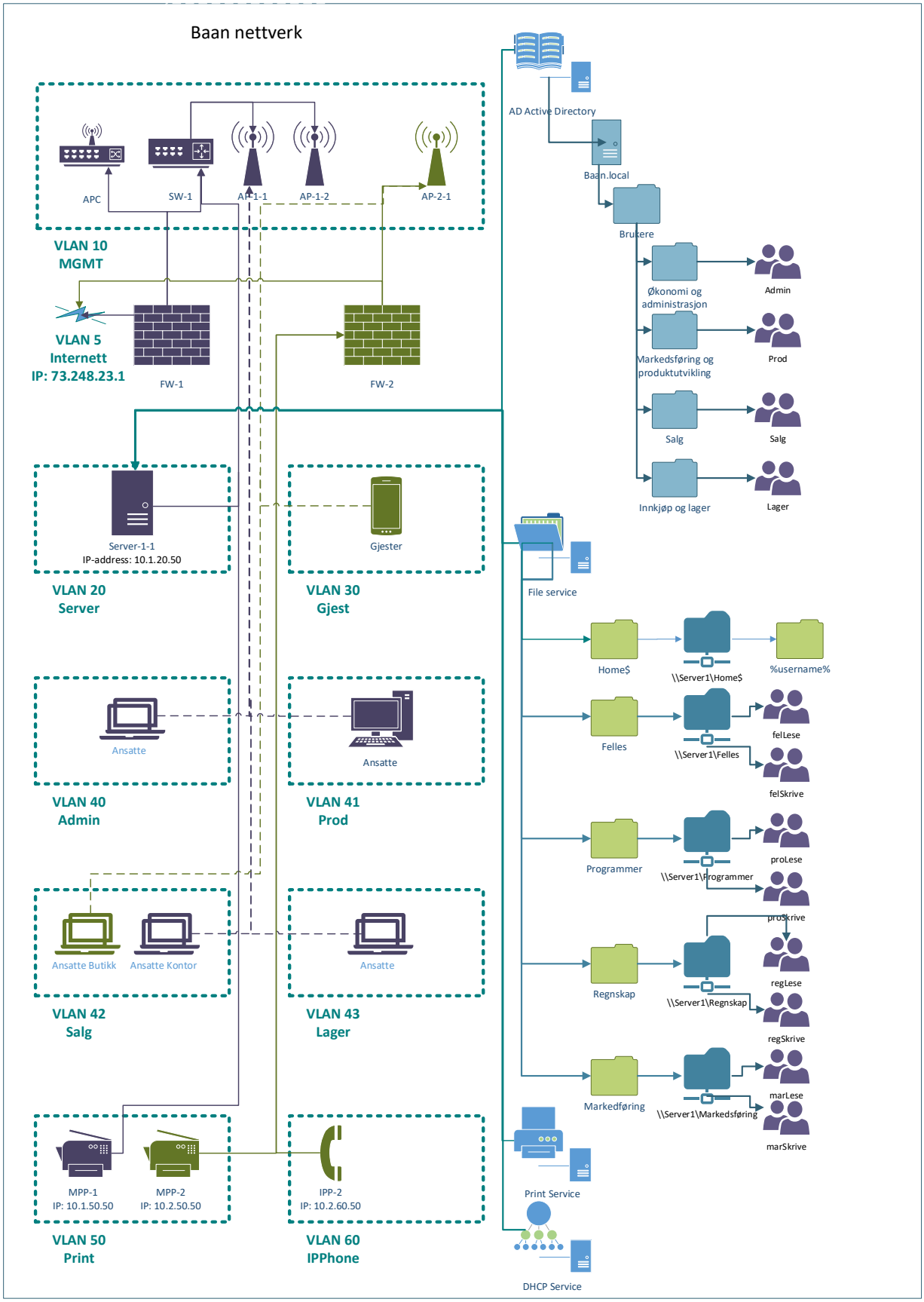
3.1 Budsjett for 2-Bånsull Butikk: Nettverk

Alt utstyr er hentet fra Dustin, med unntak av brannmur.

2-Bånsull BUT: Nettverkskostnader						
Enhet	Enhetsnavn	Enhetspris		Antall	Total	
Brannmur	Palo Alto Networks PA-440	kr	14 627,00	1	kr	14 627,00
Brannmur Bundle	PA-440, Professional Subscription Bundle (Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security), 5 years (60 months) term	kr	13 185,00	1	kr	13 185,00
Brannmur Support	PA-440, Partner enabled premium support, 5 years (60 months), term, renewal.	kr	28 107,00	1	kr	28 107,00
Access Point	Ubiquiti UniFi U6 Pro Access Point	kr	1 719,00	2	kr	3 438,00
Printer	HP Color LaserJet Pro M282nw A4 MFP	kr	3 639,00	1	kr	3 639,00
Ethernet-0.5m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	72,00	2	kr	144,00
Ethernet-1m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	114,00	4	kr	456,00
Ethernet-2m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	125,00	4	kr	500,00
Ethernet-5m	TP-Cable UTP Unshielded Lszh RJ45 5m Grey RJ-45 RJ-45 CAT 6 Grey	kr	153,00	2	kr	306,00
			Total:		**kr**	**64 402,00**
			Avskrivning over tre år:		**kr**	**21 467,33**

4 Nettverk

4.1 Oversikt over nettverket



4.2 VLAN og IP-oversikt

I nettverkskonfigurasjonen er det essensielt å segmentere ulike behov i VLAN for å tydelig skille mellom klienter, printere og servere. Dette gir mulighet for implementering av effektiv tilgangskontroll gjennom bruk av ACL-lister eller brannmur, spesielt mellom de varierte IP-nettene tilknyttet hvert VLAN. Videre anbefales det å opprette minst ett VLAN for internett og ett for MGMT (Management) for administrasjon. Det er viktig å merke seg at VLAN 1 er satt som native VLAN og bør unngås av to grunner; switchene bruker ofte dette VLAN-et for kommunikasjon mellom seg, og på mange switcher er alle portene meldt inn i VLAN 1.

4.3 Liste over VLAN

Navn	**VLAN ID**	**Beskrivelse**
Default	1	Default VLAN. Skal ikke røres.
Internet	5	VLAN mellom internet-ruter og lag3-switch
MGMT	10	Management; Rutere og annet nettverksutstyr
Server	20	Servere
Gjest	30	Gjestenettverk, begrenset
Admin	40	Økonomi og administrasjon
Prod	41	Markedsføring og produktutvikling
Salg	42	Salg
Lager	43	Innkjøp og lager
Print	50	Printere, kopimaskiner
IPPhone	60	IP mobiler

5 Serveroppsett

5.1 Active Directory

5.1.1 Brukergrupper

Navn	Gruppenavn (AD)	AD Gruppe	Medlem av
Økonomi og administrasjon	B_Admin	Global Security Group	Felles Skrive Programmer Skrive Regnskap Skrive Markedsføring Skrive
Markedsføring og produktutvikling	B_Prod	Global Security Group	Felles Skrive Programmer Lese Markedsføring Skrive
Salg	B_Salg	Global Security Group	Felles Skrive Programmer Lese Regnskap Skrive Markedsføring Lese
Innkjøp og lager	B_Lager	Global Security Group	Felles Skrive Programmer Lese Regnskap Skrive Markedsføring Lese

5.1.2 Rettighetsgrupper

Navn	Gruppenavn (AD)	AD Gruppe	Tilhørende rettigheter
Felles Lese	R_Fel_Lese	Domain Local Security Group	\\Server 1-1\Felles\ Read&Execute
Felles Skrive	R_Fel_Skrive	Domain Local Security Group	\\Server 1-1\Felles\ Modify
Programmer Lese	R_Pro_Lese	Domain Local Security Group	\\Server 1-1\Programmer\ Read&Execute
Programmer Skrive	R_Pro_Skrive	Domain Local Security Group	\\Server 1-1\Programmer\ Modify
Regnskap Lese	R_Reg_Lese	Domain Local Security Group	\\Server 1-1\Regnskap\ Read&Execute
Regnskap Skrive	R_Reg_Skrive	Domain Local Security Group	\\Server 1-1\Regnskap\ Modify
Markedsføring Lese	R_Mar_Lese	Domain Local Security Group	\\Server 1-1\Markedsføring\ Read&Execute
Markedsføring Skrive	R_Mar_Skrive	Domain Local Security Group	\\Server 1-1\Markedsføring\ Modify

5.2 Liste over brukere

Fullt navn	Brukernavn	Avdeling	Arbeidsstasjon
Anne Hansen	annhan	Økonomi og administrasjon	Bærbar
Bjørn Olsen	bjools	Markedsføring og produktutvikling	Stasjonær
Carl Andersson	carand	Salg	Bærbar
David Nilsen	davnil	Innkjøp og lager	Bærbar
Emma Berg	emmber	Salg	Bærbar
Fredrik Møller	fremol	Salg	Bærbar
Greta Petersen	grepet	Salg	Bærbar
Håkon Jansen	hakjan	Salg	Bærbar

5.3 Fildeling og hjemmeområde

I Bånsull implementerer vi en mappestruktur med "Home$" som hjemmeområde. Under denne opprettes følgende undermapper: Felles, Programmer, Regnskap, Markedsføring og individuelle hjemmeområder for hver bruker, som "%username%». Dette gir en organisert og strukturert filoppsett, med dedikerte områder for felles ressurser og spesifikke områder for ulike brukere.

5.4 Gruppepolicier

For å forbedre sikkerheten til brukernes passord i systemet, implementerer vi bestemte standarder basert på CIS Controls for Windows 10 Benchmark, som er en anbefalt og oppdatert sikkerhetsstandard. For mer informasjon om hvert enkelt krav, se hvert punkt i Benchmark. Policiene under er et eksempel på CIS nivå 1; et minimum nivå for sikkerhetshygiene. I tillegg til å sikre maskinene på nettverket, er det også viktig å sikre domenekontrollere med CIS Control.[8]

5.4.1 Passordpolicy

- 1.1.1 'Enforce password history' er satt til 24
- 1.1.2 'Maximum password age' er satt til 365
- 1.1.3 'Minimum password age' er satt til 1
- 1.1.4 'Mimimum password length' er satt til 15
- 1.1.5 'Password must meet complexity requirements' er aktivert
- 1.1.6 'Relax minimum password length limits' er aktivert
- 1.1.7 'Store passwords using reversible encryption' er deaktivert

[8] CIS Controls – Windows 10 og Windows Server 2022 Benchmark

5.4.2 Kontosperrepolicy

- 1.2.1 'Account lockout duration' er satt til 15 minutter
- 1.2.2 'Account lockout threshold' er satt til 5 ugyldige påloggingsforsøk
- 1.2.3 'Allow Administrator account lockout' er aktivert
- 1.2.4 'Reset account lockout counter after' er satt til 15 minutter

5.5 Skriverinstillinger

I nettverket har vi implementert funksjonalitet for skrivere som støtter både A4- og A3-formater, samt standard svart-hvitt-utskrift med mulighet for farger. Dette tar sikte på å imøtekomme ulike behov innenfor dokumentutskrift, og gir brukerne fleksibilitet til å velge det optimale formatet og farge basert på deres krav.

I tillegg har vi en skriverkø med en gruppepolicy for å regulere tilgangen til skriveren. Denne tilnærmingen bidrar til en mer strukturert og effektiv administrasjon av utskriftsoppgaver ved å organisere og prioritere utskriftene. Med en sentralisert tilnærming kan vi bedre håndtere og overvåke utskriftsprosessene, samtidig som vi sikrer at ressursene utnyttes optimalt.

V vil også integrere skriverne med Print Service på serveren. Dette sentraliserte systemet gir oss muligheten til å enkelt administrere skrivere. Denne metoden til utskrifts bidrar til å forbedre effektiviteten og påliteligheten til utskriftsprosessene i hele nettverket.

5.6 DHCP-pool

Alle pools på nettverket skal starte på 50 og ende på 250, for å gjøre plass for eventuelt utstyr som krever statisk IP. Dette kan variere, men kan inkludere verktøy for scann av nettverk, en brannmur med flere noder, og mer.

- **Subnet mask**: 255.255.255.0
- **DNS Intern**: 10.1.20.2
- **DNS for gjest**: 1.1.1.1 og 1.0.0.1

1-Bånsull Kontor				
Navn på scope	**VLAN-ID**	**Start IP-address**	**End IP-address**	**Gateway**
Gjest	30	10.2.30.50	10.2.30.250	10.2.30.1
Admin	40	10.1.40.50	10.1.40.250	10.1.40.1
Prod	41	10.1.41.50	10.1.41.250	10.1.41.1
Salg	42	10.1.42.50	10.1.42.250	10.1.42.1
Lager	43	10.1.43.50	10.1.43.250	10.1.43.1
IPPhone	60	10.1.60.50	10.1.60.250	10.1.60.1

Daniel

2-Bånsull Butikk				
Navn på scope	**VLAN-ID**	**Start IP-address**	**End IP-address**	**Gateway**
Gjest	30	10.2.30.50	10.2.30.250	10.2.30.1
Prod	41	10.1.41.50	10.1.41.250	10.1.41.1
Salg	42	10.1.42.50	10.1.42.250	10.1.42.1
IPPhone	60	10.2.60.50	10.2.60.250	10.2.60.1

6 Avslutning

Dette nettverksoppsettet følger samme mal som dokumentet angående VLAN-oppsett. Målet var å gjøre det så likt til et ekte bedriftsdokument som mulig. På den måten kan jeg også benytte det som referanse senere.

Med dette fulgte en del utfordringer, som budsjett og moms, spesielt utstyrsstandarder, hvor jeg ikke har noen erfaring. En annen utfordring kom med Windows 10 Benchmarks og NSMs grunnprinsipper for IKT-sikkerhet, hvor begge inkluderer mange potensielle polices. Disse må da begrunnes og kartlegges.

Alt i alt har jeg lært mye om dokument standarder – spesifikt det å benytte Grunnprinsipper for IKT til nettverksdokumenter - sikkerhetsrammeverk og igjen gått gjennom oppsett av Windows server som domenekontroller, DHCP-, DNS-, fil- og printserver.